

# Exhibit 1



US008677116B1

(12) **United States Patent**  
**Bicer**(10) **Patent No.:** **US 8,677,116 B1**  
(45) **Date of Patent:** **Mar. 18, 2014**(54) **SYSTEMS AND METHODS FOR AUTHENTICATION AND VERIFICATION**(71) Applicant: **Jack Bicer**, Irvine, CA (US)(72) Inventor: **Jack Bicer**, Irvine, CA (US)

(\*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **13/963,941**(22) Filed: **Aug. 9, 2013**

2010/0273527 A1	10/2010	Silverbrook et al.
2011/0071895 A1	3/2011	Masri
2011/0125561 A1	5/2011	Marcus
2011/0137742 A1*	6/2011	Parikh ..... 705/26.1
2011/0137797 A1	6/2011	Stals et al.

(Continued)

**FOREIGN PATENT DOCUMENTS**

EP	1197046 A1	4/2002
GB	2481663 B2	6/2012

(Continued)

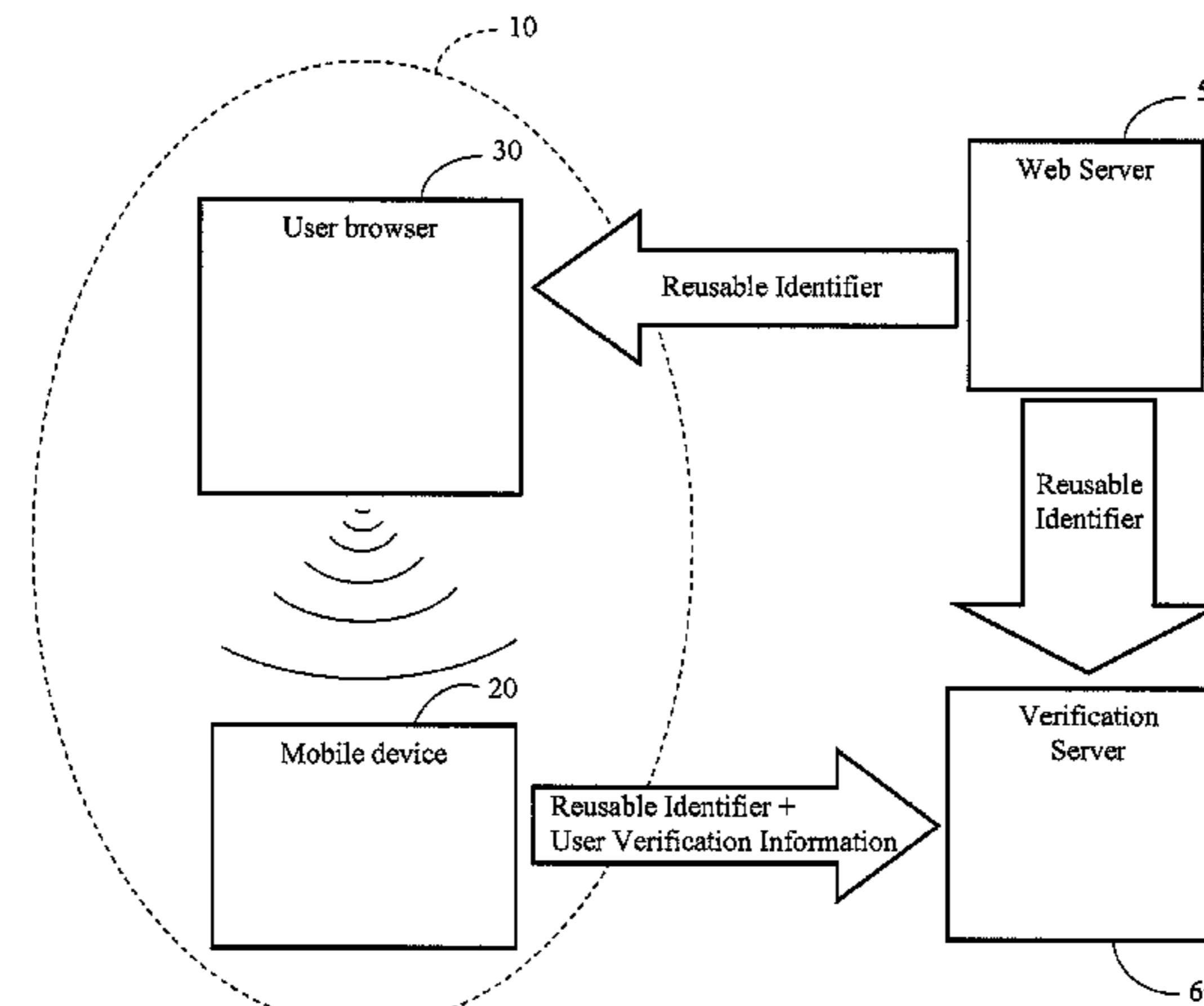
**OTHER PUBLICATIONS**

<http://www.calvin-c.com/blog/tag/mobile-payment> Jul. 23, 2013.

(Continued)

*Primary Examiner* — Nadia Khoshnoodi*Assistant Examiner* — Robert Leung(74) *Attorney, Agent, or Firm* — Knobbe, Martens, Olson & Bear LLP(57) **ABSTRACT**

Computer systems and methods are provided for authenticating a user seeking to conduct at least one interaction with a secured capability provided by a computer. The method includes receiving a first signal from the computer providing the secured capability. The first signal includes a reusable identifier corresponding to the secured capability. The method further includes receiving a second signal from an electronic device being used by the user. The second signal includes a copy of the reusable identifier and user verification information. The method further includes using a processor to evaluate, based at least on the first signal and the second signal, whether the user is authorized to conduct the at least one interaction with the secured capability. The method further includes, in response to an indication from the processor that the user is authorized to conduct the at least one interaction with the secured capability, transmitting a third signal including authorization information to at least one of the electronic device and the computer.

**22 Claims, 22 Drawing Sheets**

**US 8,677,116 B1**

Page 2

(56)	<b>References Cited</b>	
U.S. PATENT DOCUMENTS		
2011/0208659 A1	8/2011	Easterly et al.
2011/0212717 A1	9/2011	Rhoads et al.
2011/0219427 A1*	9/2011	Hito et al. .... 726/3
2011/0288962 A1	11/2011	Rankin, Jr. et al.
2011/0289106 A1	11/2011	Rankin, Jr. et al.
2011/0307318 A1	12/2011	LaPorte et al.
2011/0313870 A1	12/2011	Eicher et al.
2012/0012649 A1	1/2012	Hsu
2012/0078782 A1	3/2012	Schoenberg et al.
2012/0084162 A1	4/2012	Smith et al.
2012/0123841 A1	5/2012	Taveau et al.
2012/0124656 A1	5/2012	Senac
2012/0136739 A1	5/2012	Chung
2012/0150729 A1	6/2012	Isaacson et al.
2012/0158581 A1	6/2012	Cooley et al.
2012/0159591 A1	6/2012	Payne et al.
2012/0173426 A1	7/2012	Foster et al.
2012/0179527 A1	7/2012	Ball et al.
2012/0191553 A1	7/2012	Sathe et al.
2012/0191610 A1	7/2012	Prasad
2012/0203695 A1*	8/2012	Morgan et al. .... 705/44
2012/0222055 A1	8/2012	Schaefer et al.
		2012/0234907 A1* 9/2012 Clark et al. .... 235/375
		2012/0246018 A1 9/2012 Sathe et al.
		2012/0254025 A1 10/2012 Prasad
		2012/0265585 A1 10/2012 Muirbrook et al.
		2012/0267432 A1 10/2012 Kuttuva
		2012/0284130 A1 11/2012 Lewis et al.
		2012/0290480 A1 11/2012 Chen
		2012/0310757 A1 12/2012 Kim et al.
		2013/0041781 A1 2/2013 Freydberg
		2013/0054320 A1 2/2013 Dorso et al.
		2013/0060686 A1 3/2013 Mersky
		2013/0067235 A1 3/2013 Anson
FOREIGN PATENT DOCUMENTS		
WO	WO 2006/102848	10/2006
WO	WO 2007/144708	12/2007
WO	WO 2008/040949	4/2008
WO	WO 2009/116954	9/2009
WO	WO2012/069845 *	5/2013 .... H04L 29/06
OTHER PUBLICATIONS		
<a href="http://www.calvin-c.com/blog/mobile-payment">http://www.calvin-c.com/blog/mobile-payment</a> Jul. 23, 2013.		

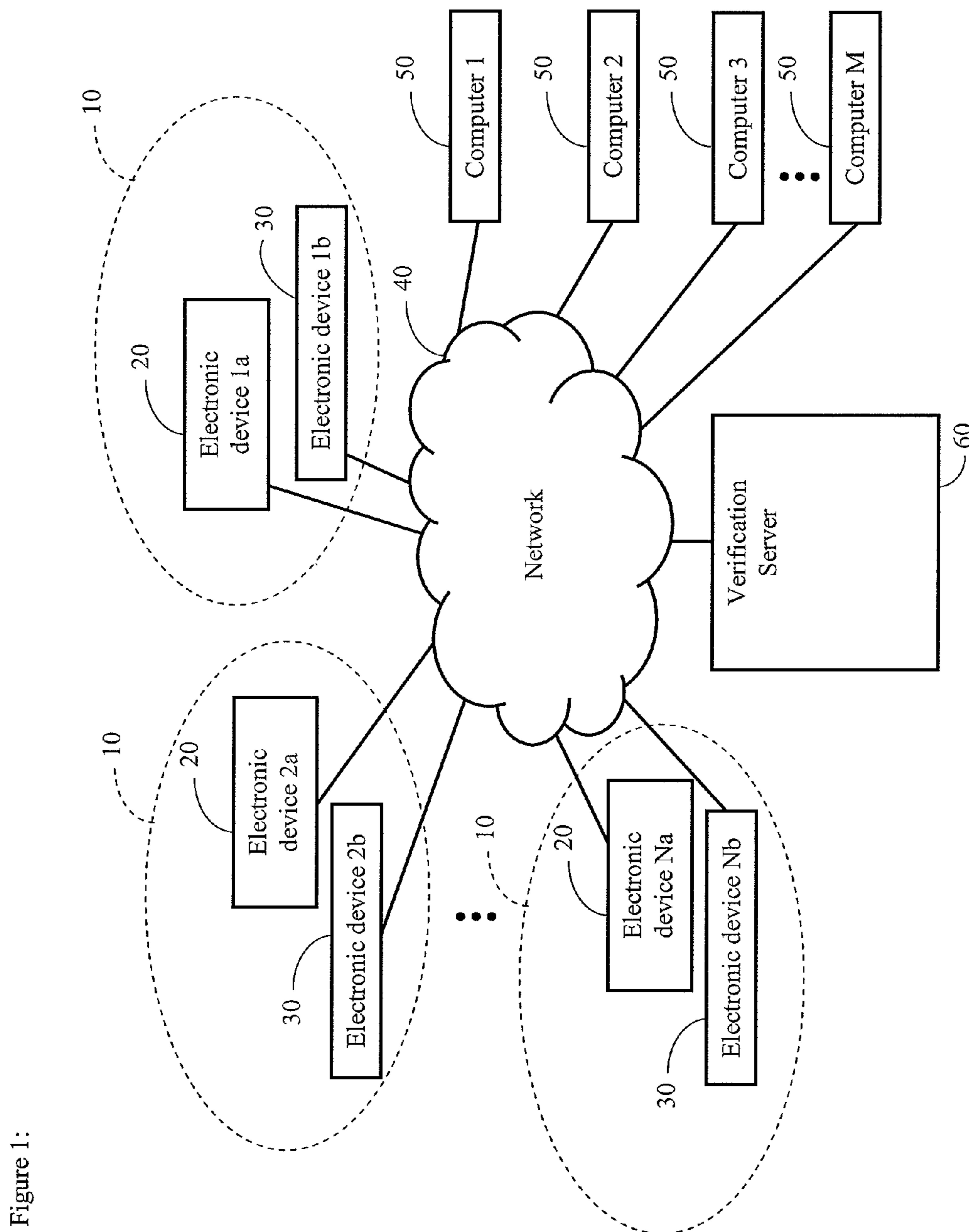
\* cited by examiner

U.S. Patent

Mar. 18, 2014

Sheet 1 of 22

US 8,677,116 B1



**U.S. Patent**

Mar. 18, 2014

Sheet 2 of 22

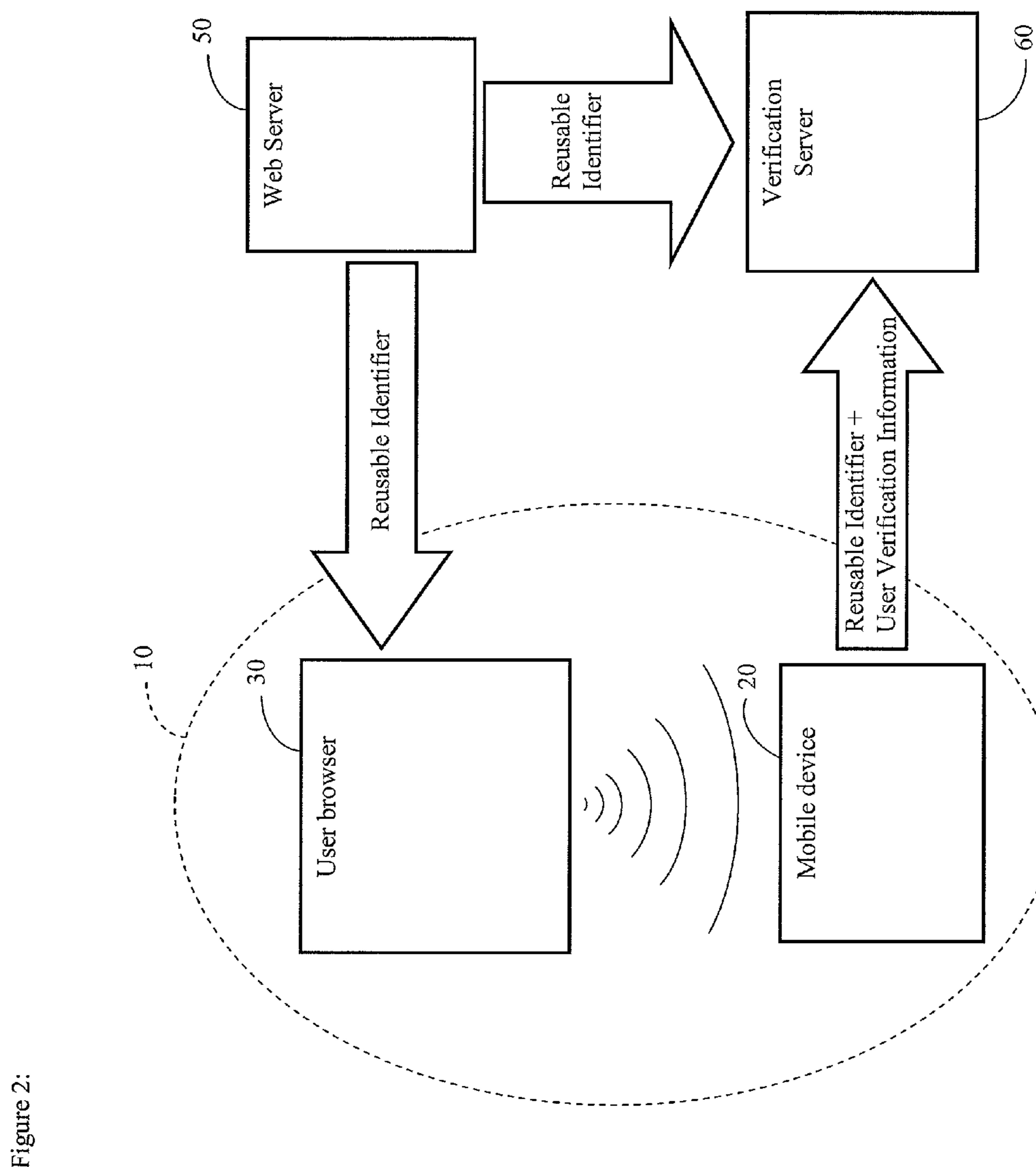
**US 8,677,116 B1**

Figure 2:

U.S. Patent

Mar. 18, 2014

Sheet 3 of 22

US 8,677,116 B1

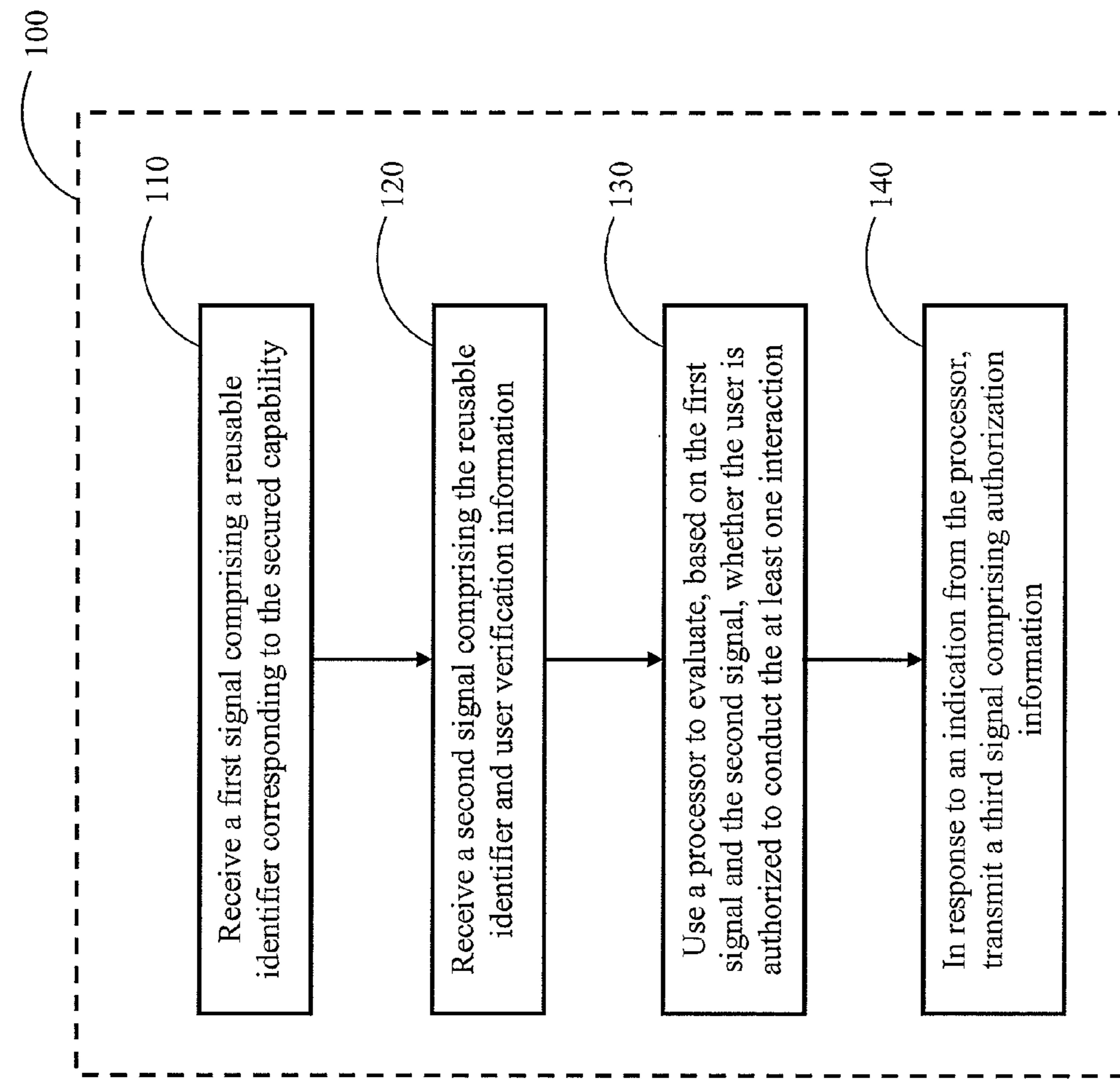


Figure 3A:

U.S. Patent

Mar. 18, 2014

Sheet 4 of 22

US 8,677,116 B1

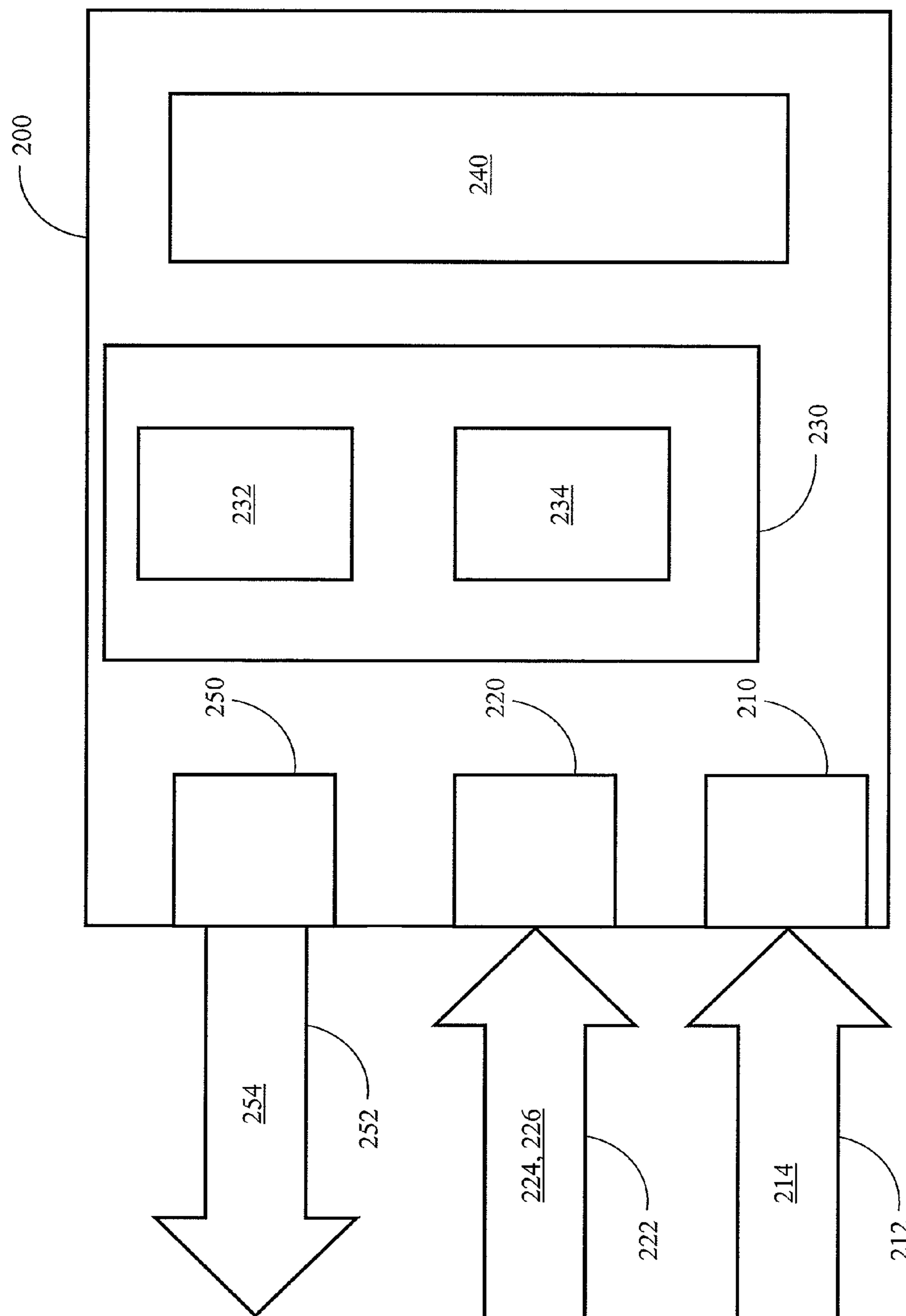


Figure 3B:

U.S. Patent

Mar. 18, 2014

Sheet 5 of 22

US 8,677,116 B1

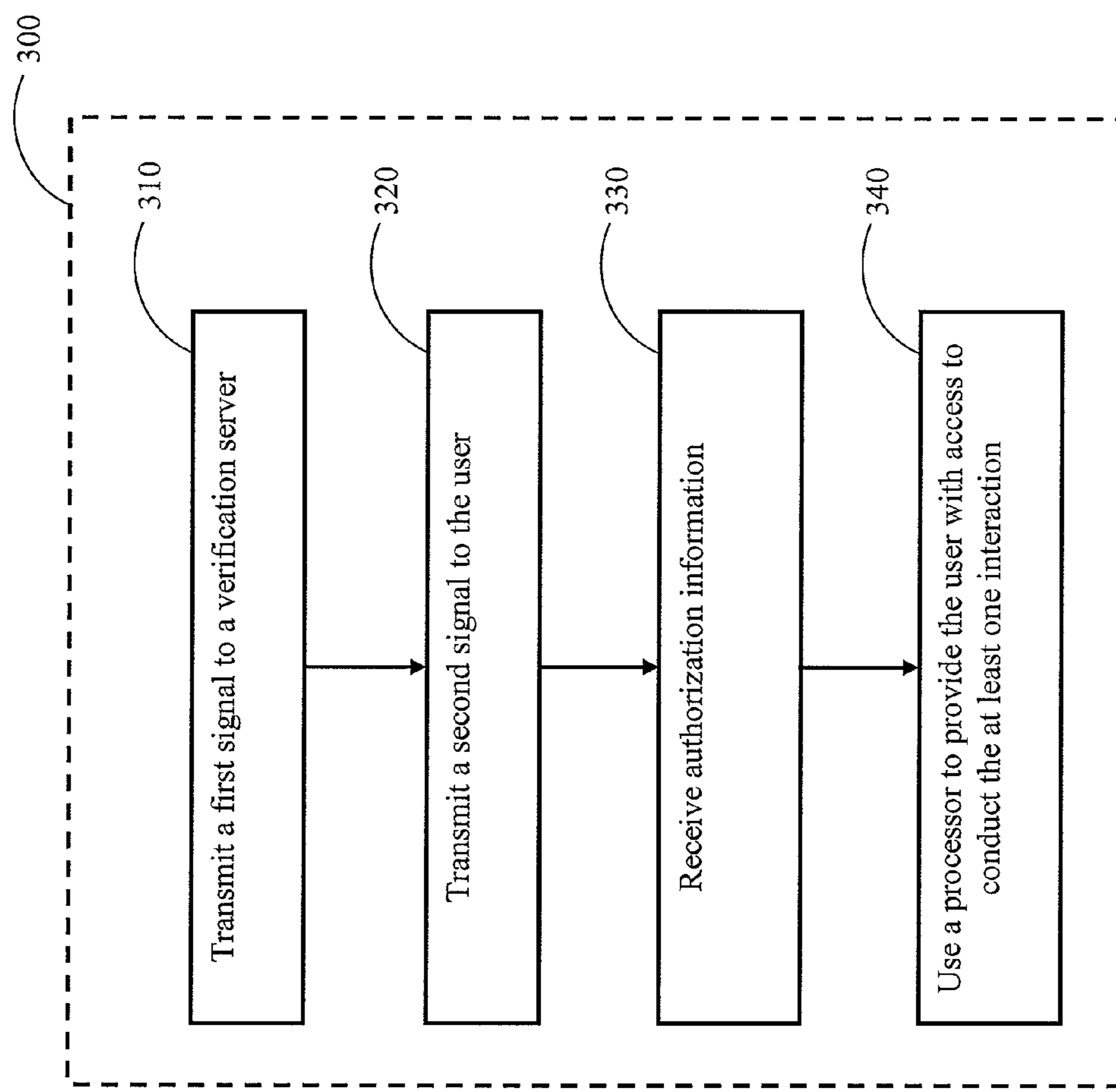
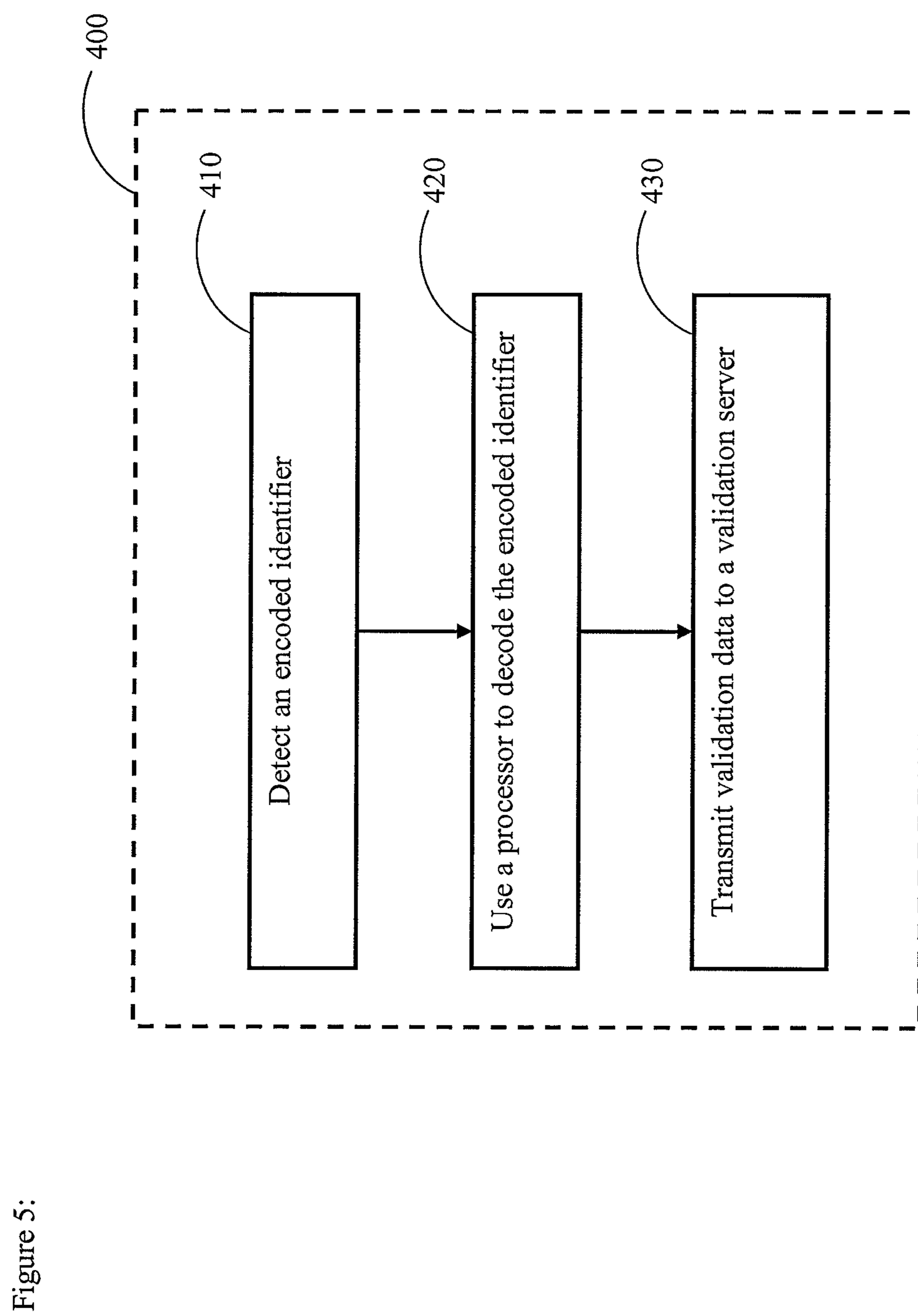


Figure 4:

**U.S. Patent**

Mar. 18, 2014

Sheet 6 of 22

**US 8,677,116 B1**

U.S. Patent

Mar. 18, 2014

Sheet 7 of 22

US 8,677,116 B1

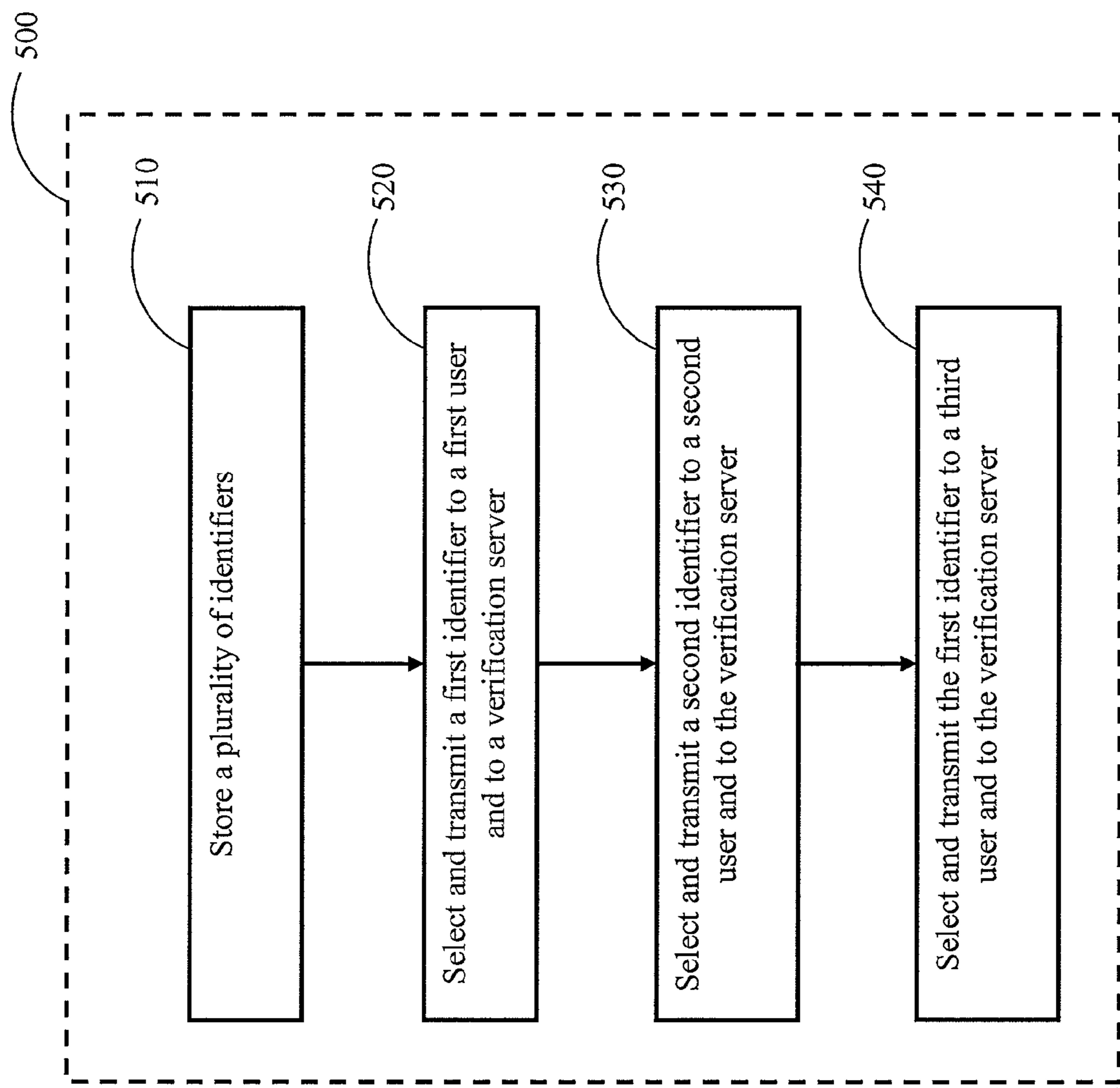


Figure 6:

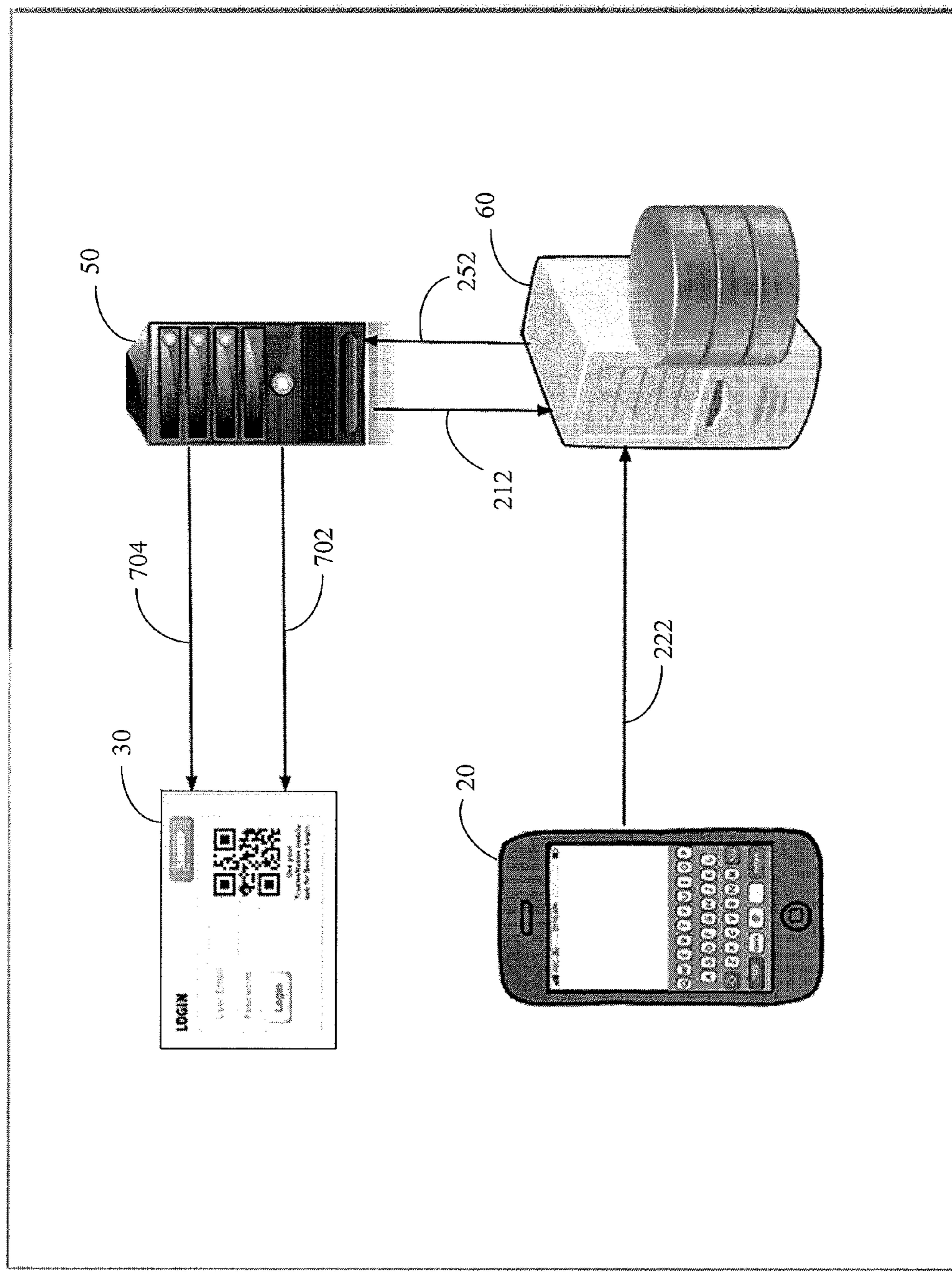
U.S. Patent

Mar. 18, 2014

Sheet 8 of 22

US 8,677,116 B1

Figure 7:



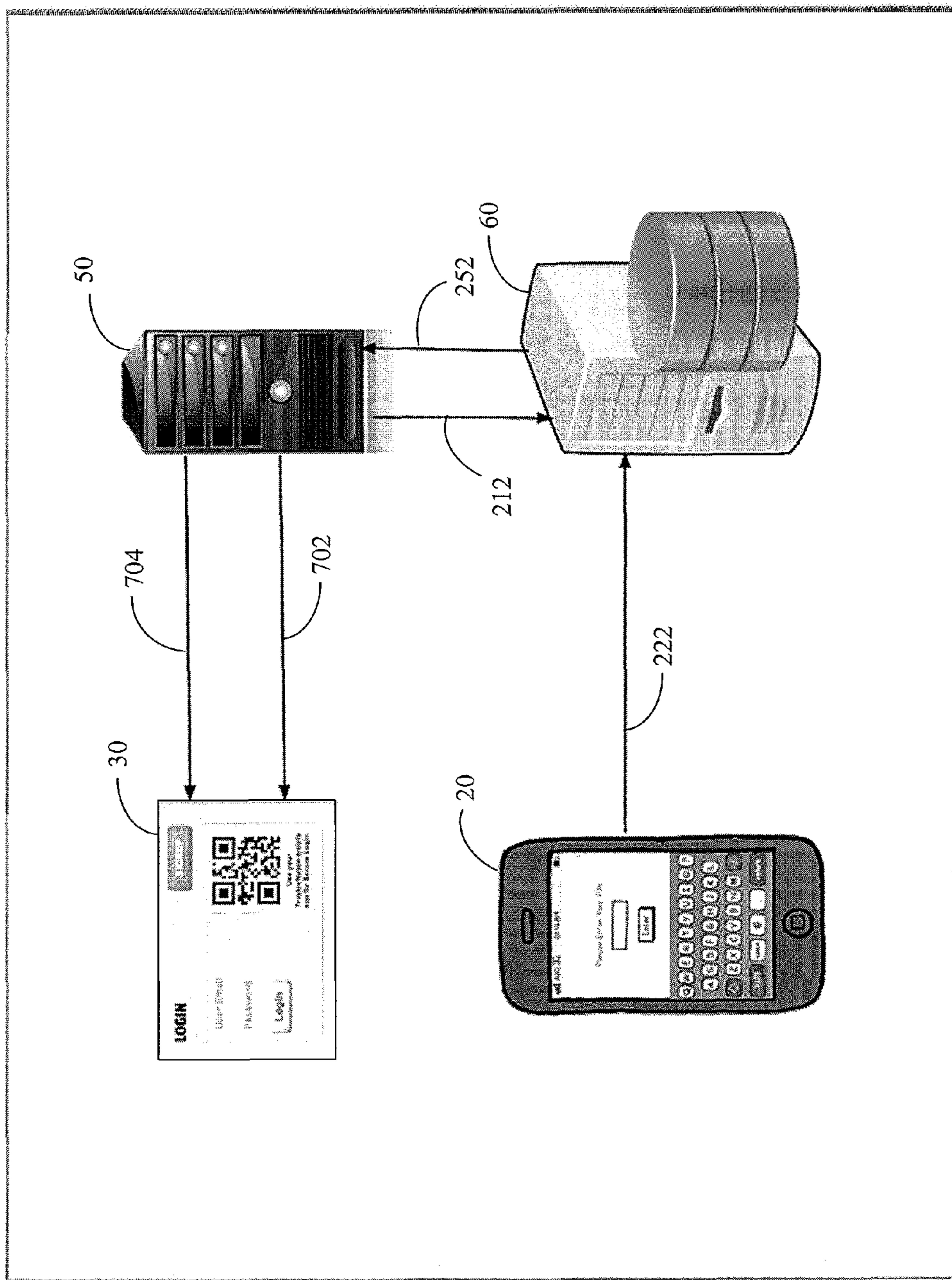
U.S. Patent

Mar. 18, 2014

Sheet 9 of 22

US 8,677,116 B1

Figure 8:

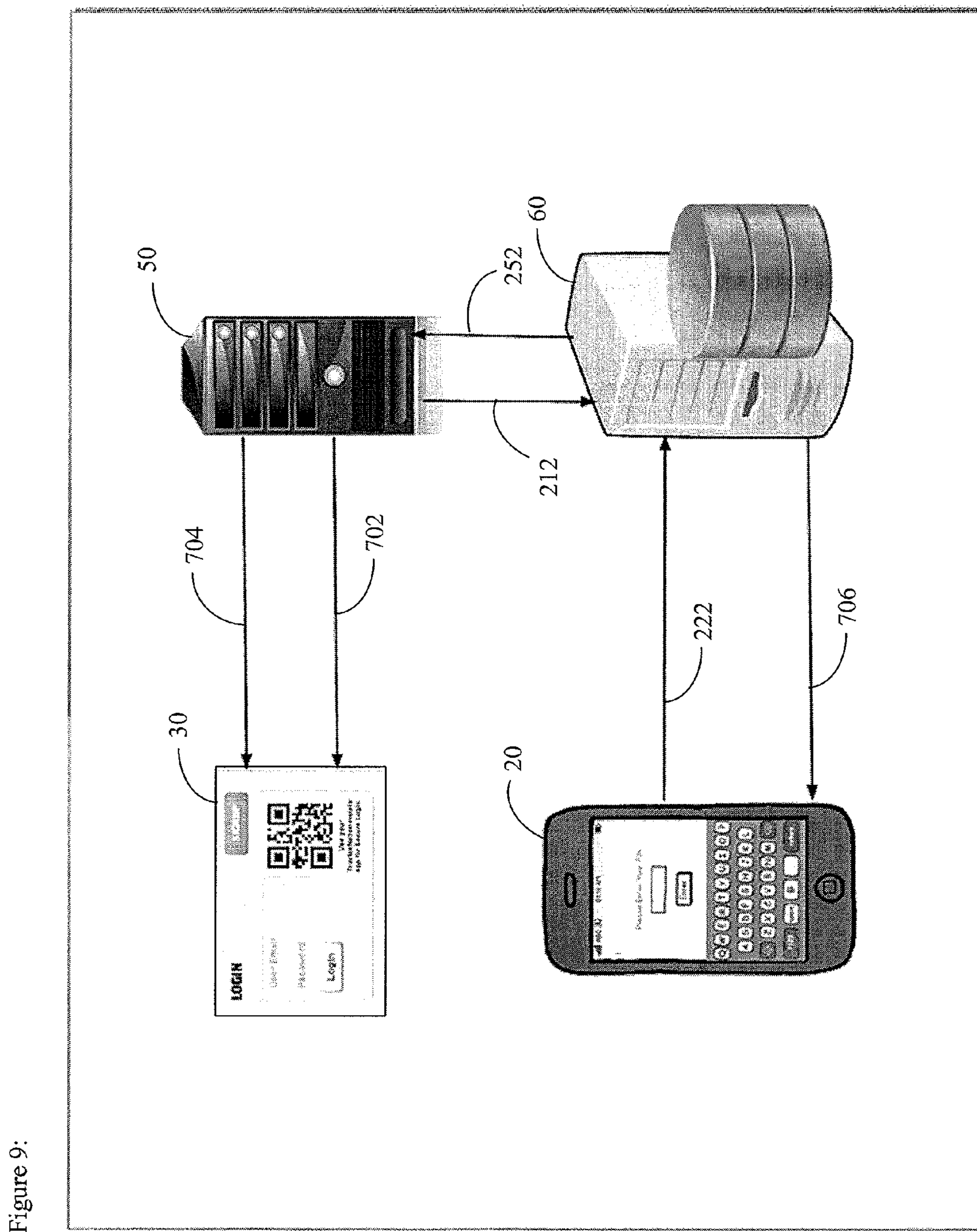


U.S. Patent

Mar. 18, 2014

Sheet 10 of 22

US 8,677,116 B1



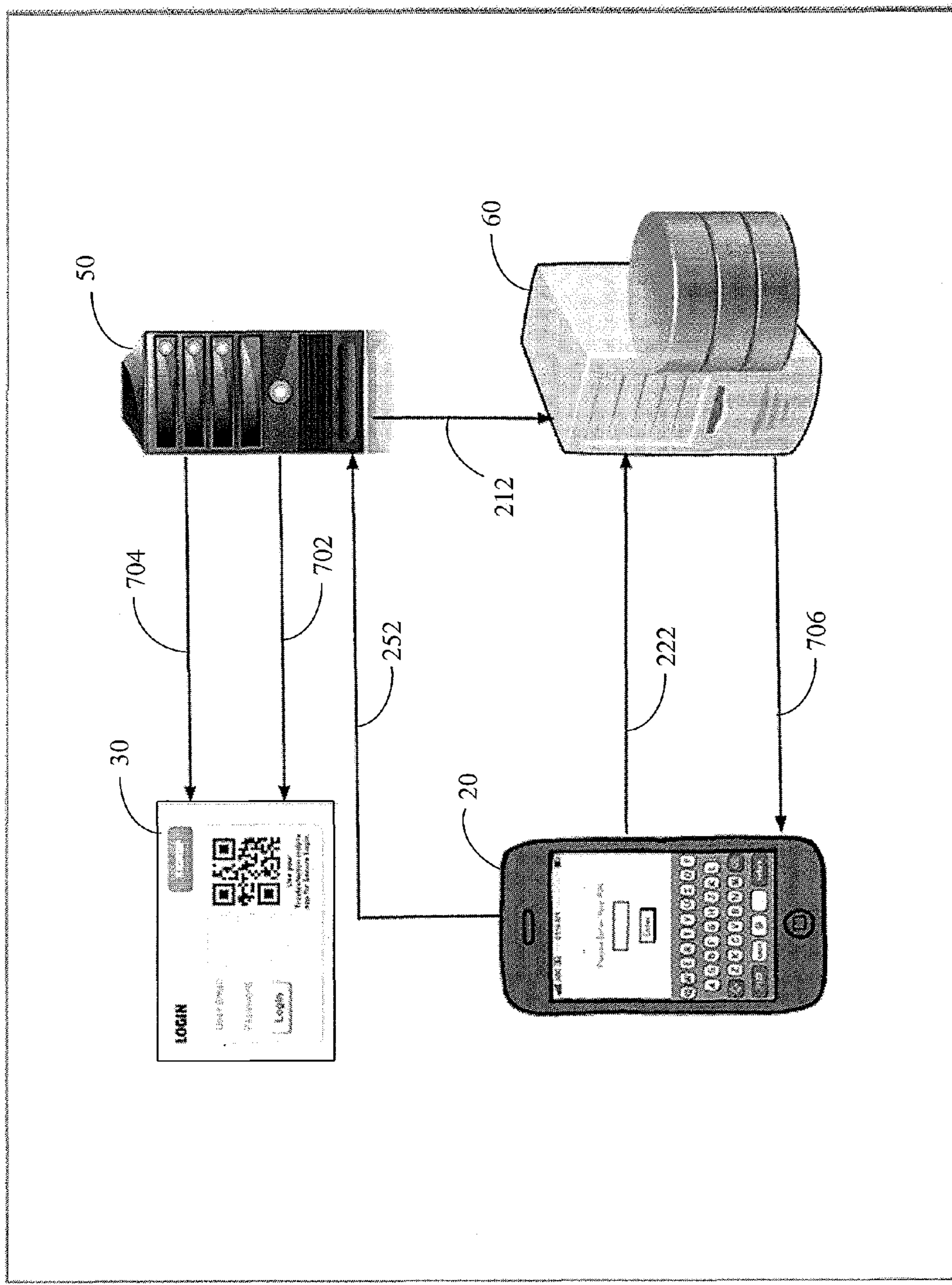
U.S. Patent

Mar. 18, 2014

Sheet 11 of 22

US 8,677,116 B1

Figure 10:



U.S. Patent

Mar. 18, 2014

Sheet 12 of 22

US 8,677,116 B1

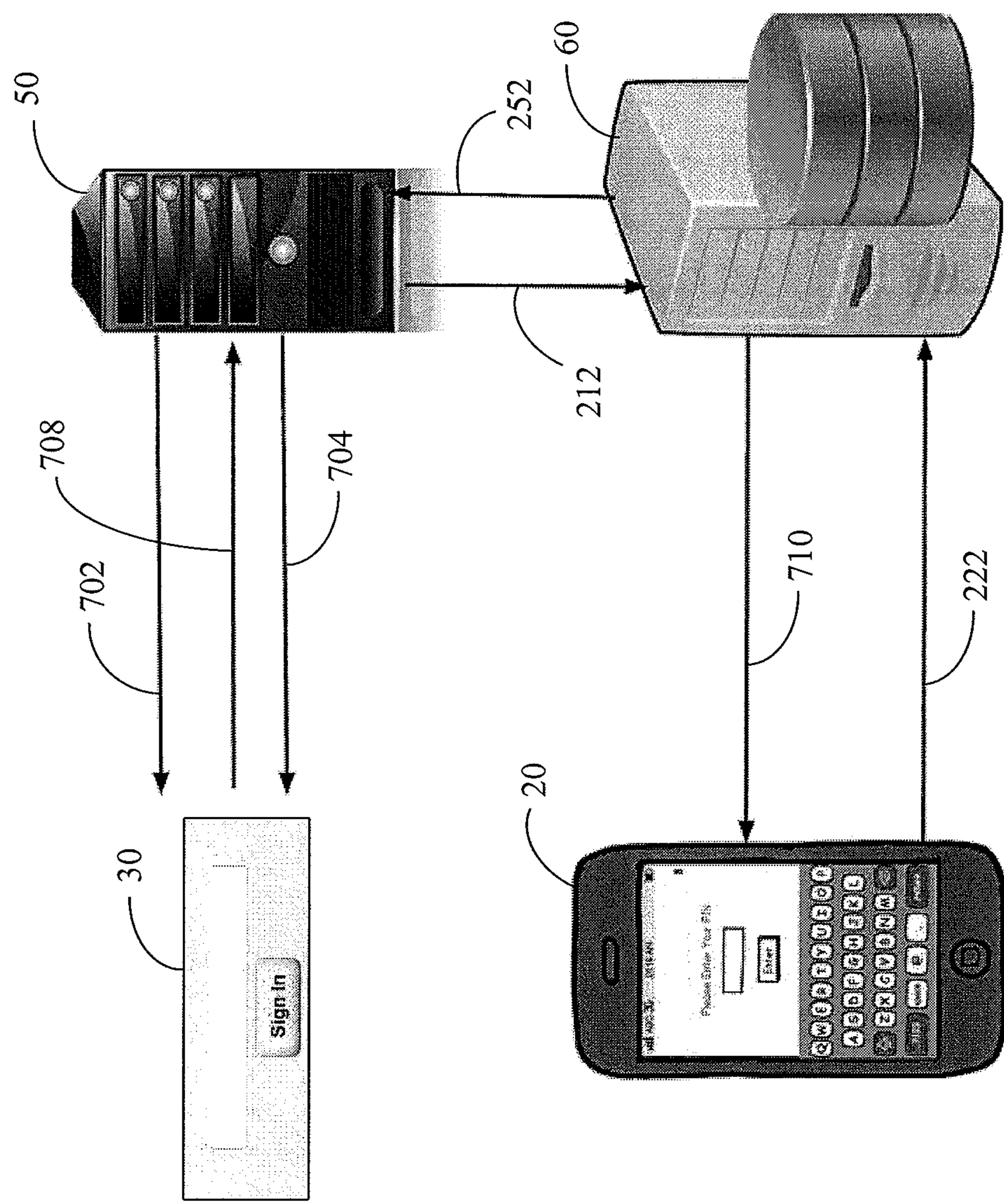


Figure 11:

U.S. Patent

Mar. 18, 2014

Sheet 13 of 22

US 8,677,116 B1

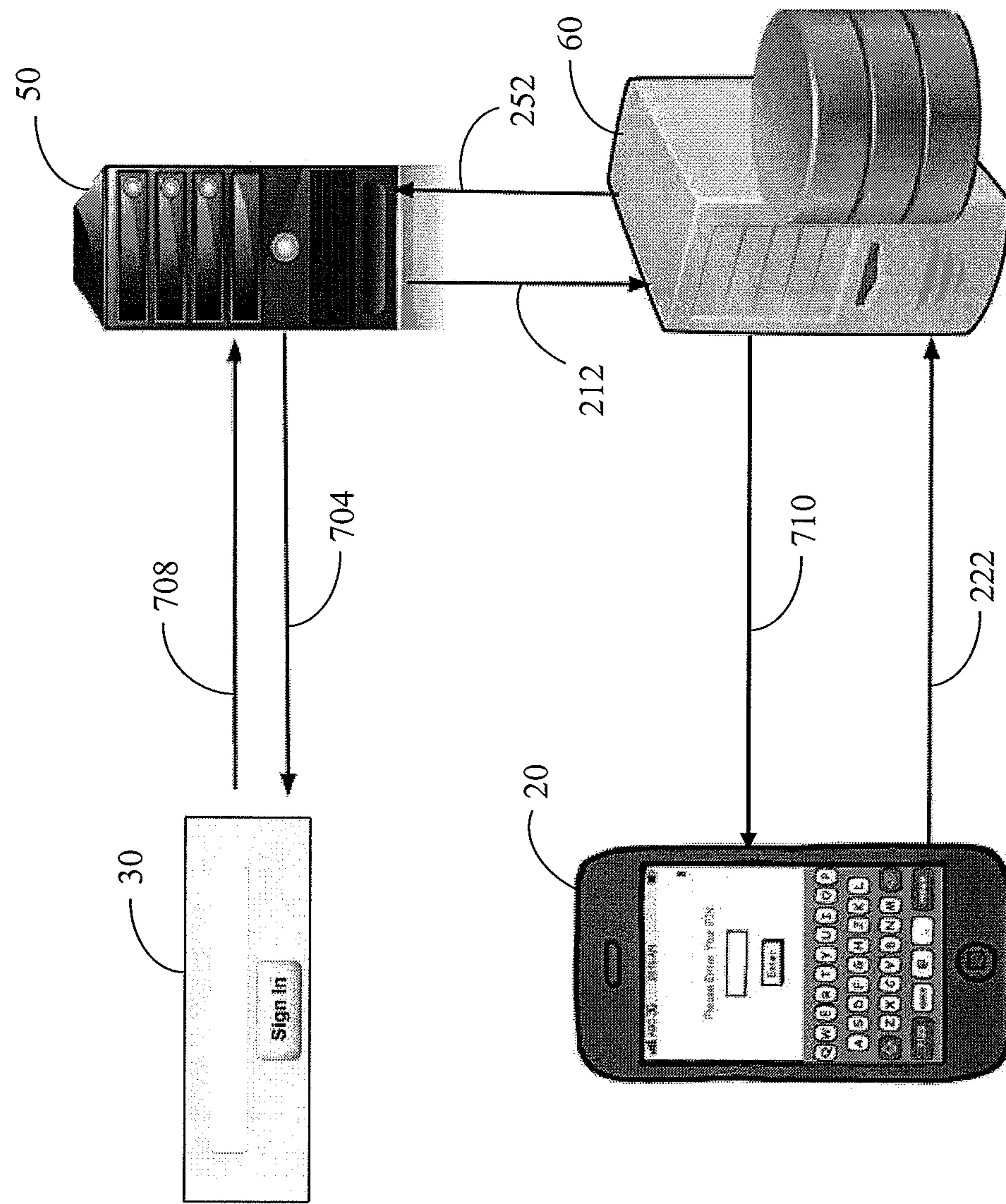


Figure 12:

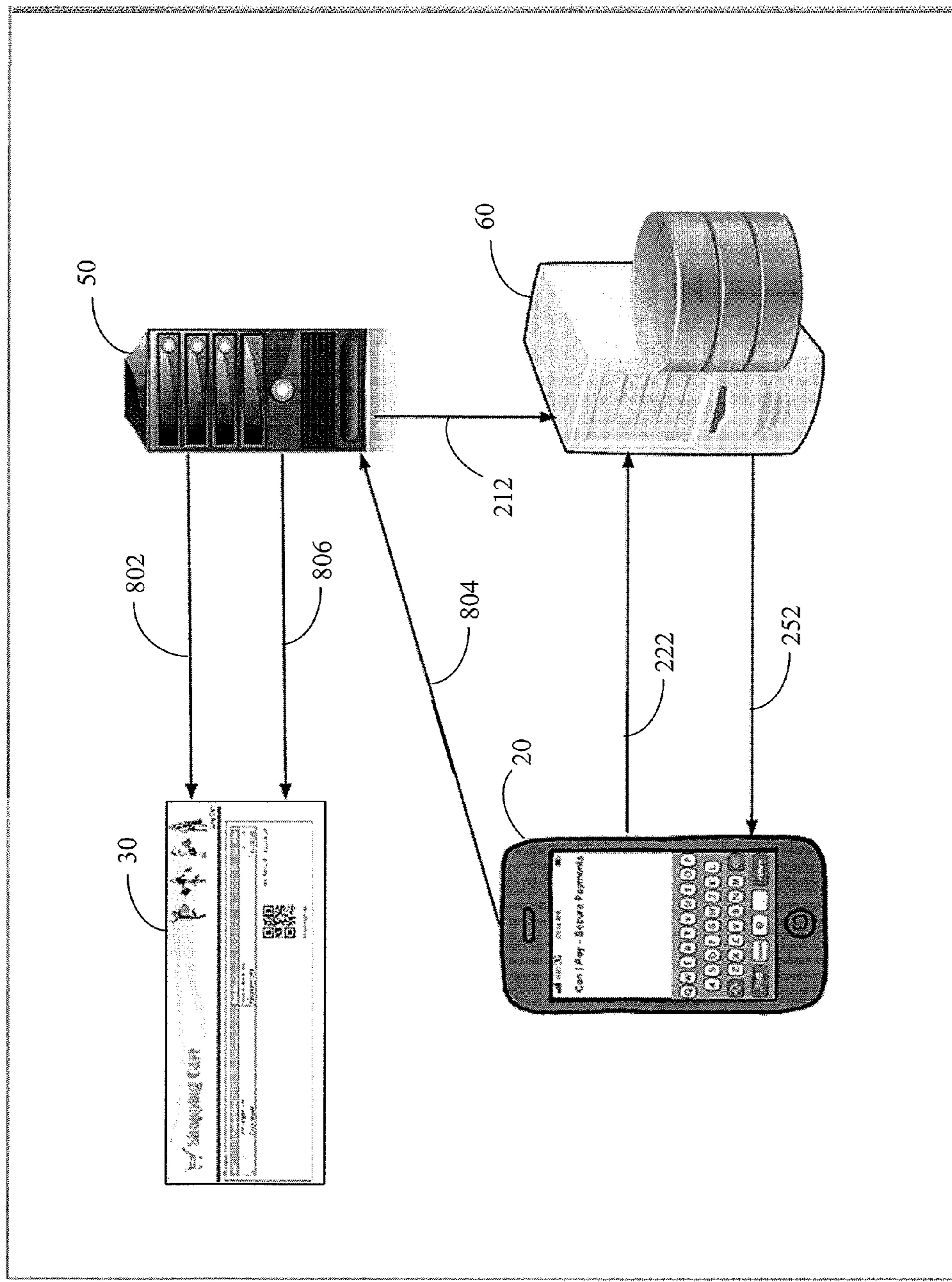
U.S. Patent

Mar. 18, 2014

Sheet 14 of 22

US 8,677,116 B1

Figure 13:



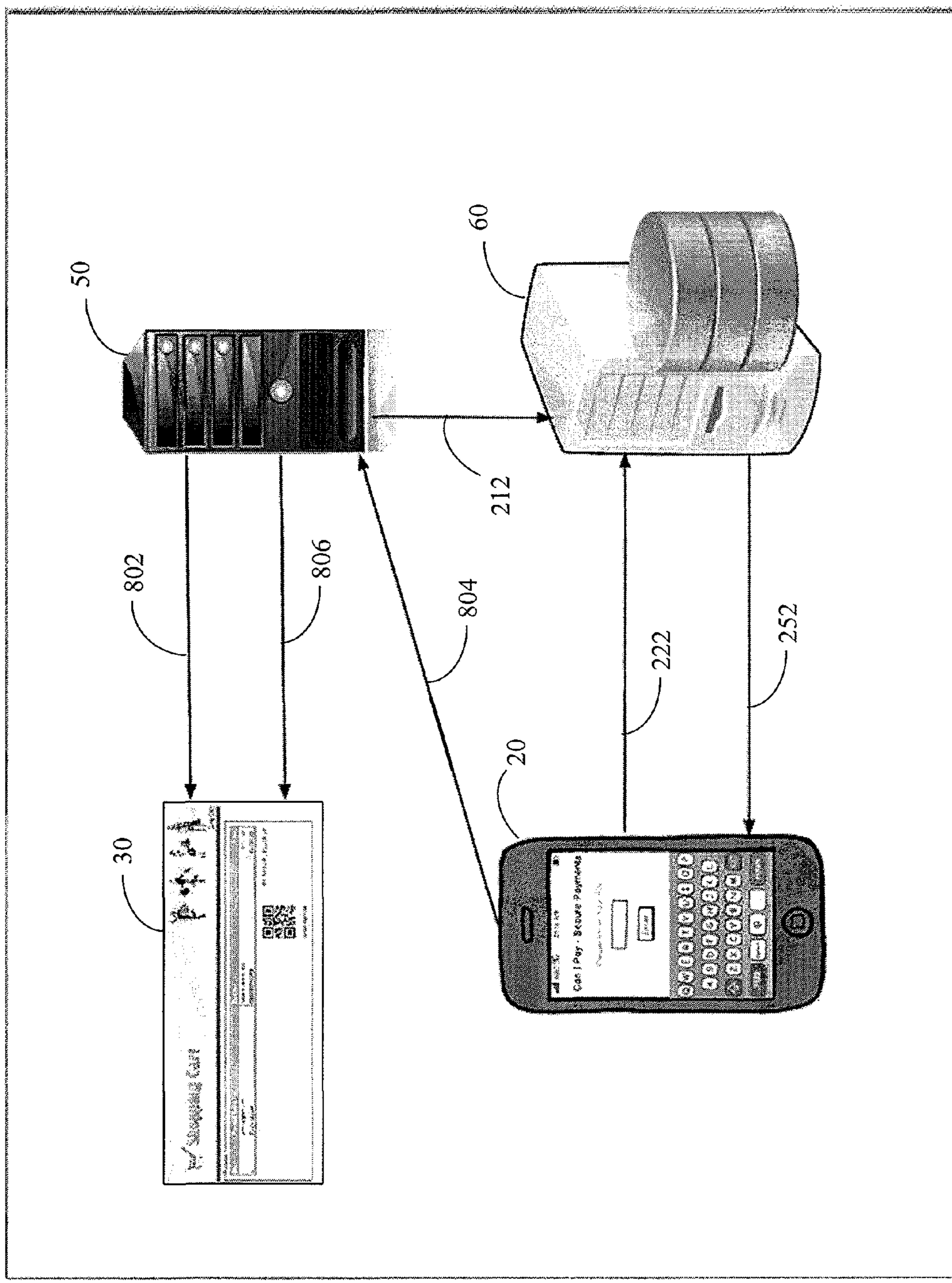
U.S. Patent

Mar. 18, 2014

Sheet 15 of 22

US 8,677,116 B1

Figure 14:



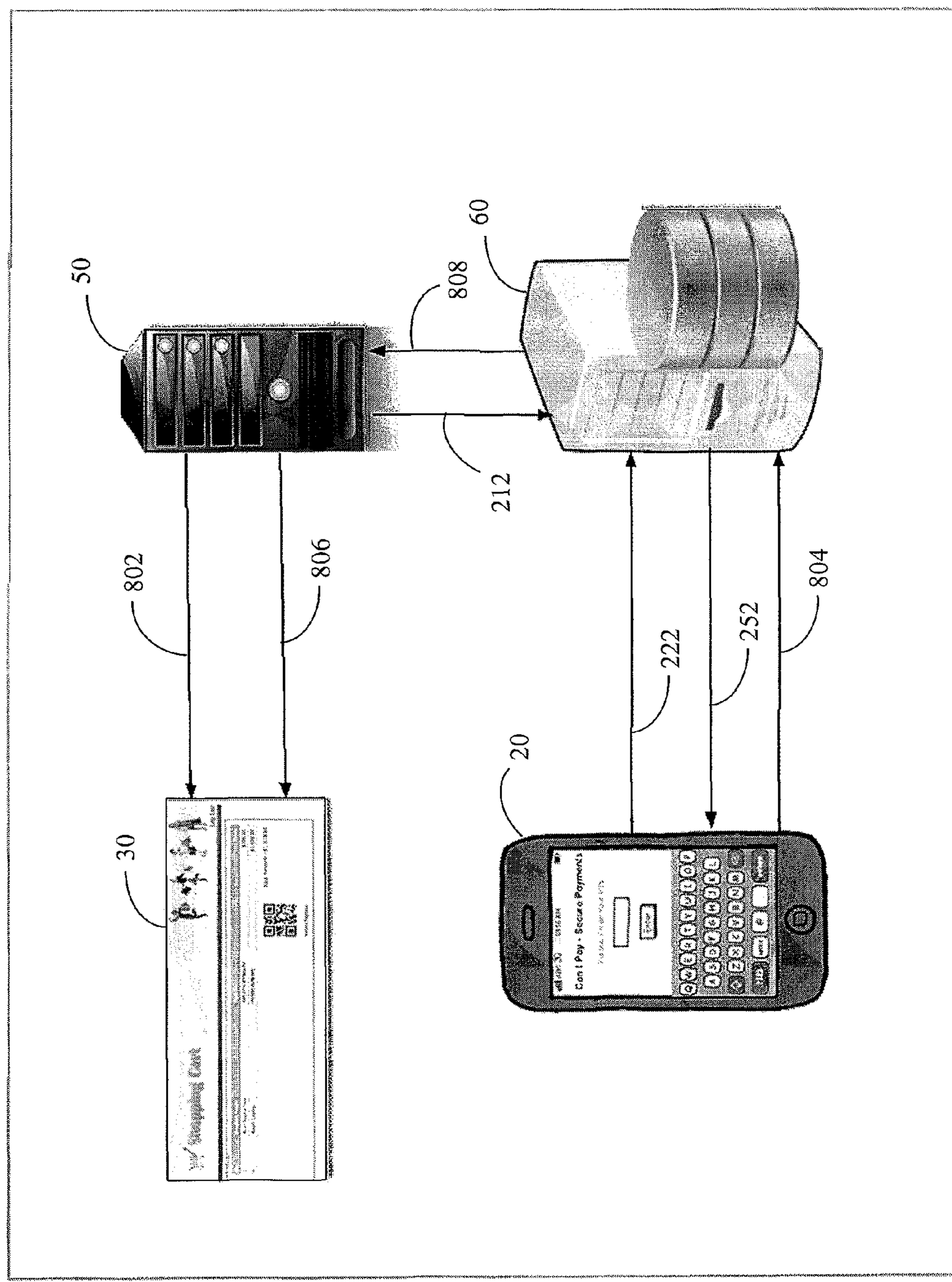
U.S. Patent

Mar. 18, 2014

Sheet 16 of 22

US 8,677,116 B1

Figure 15:

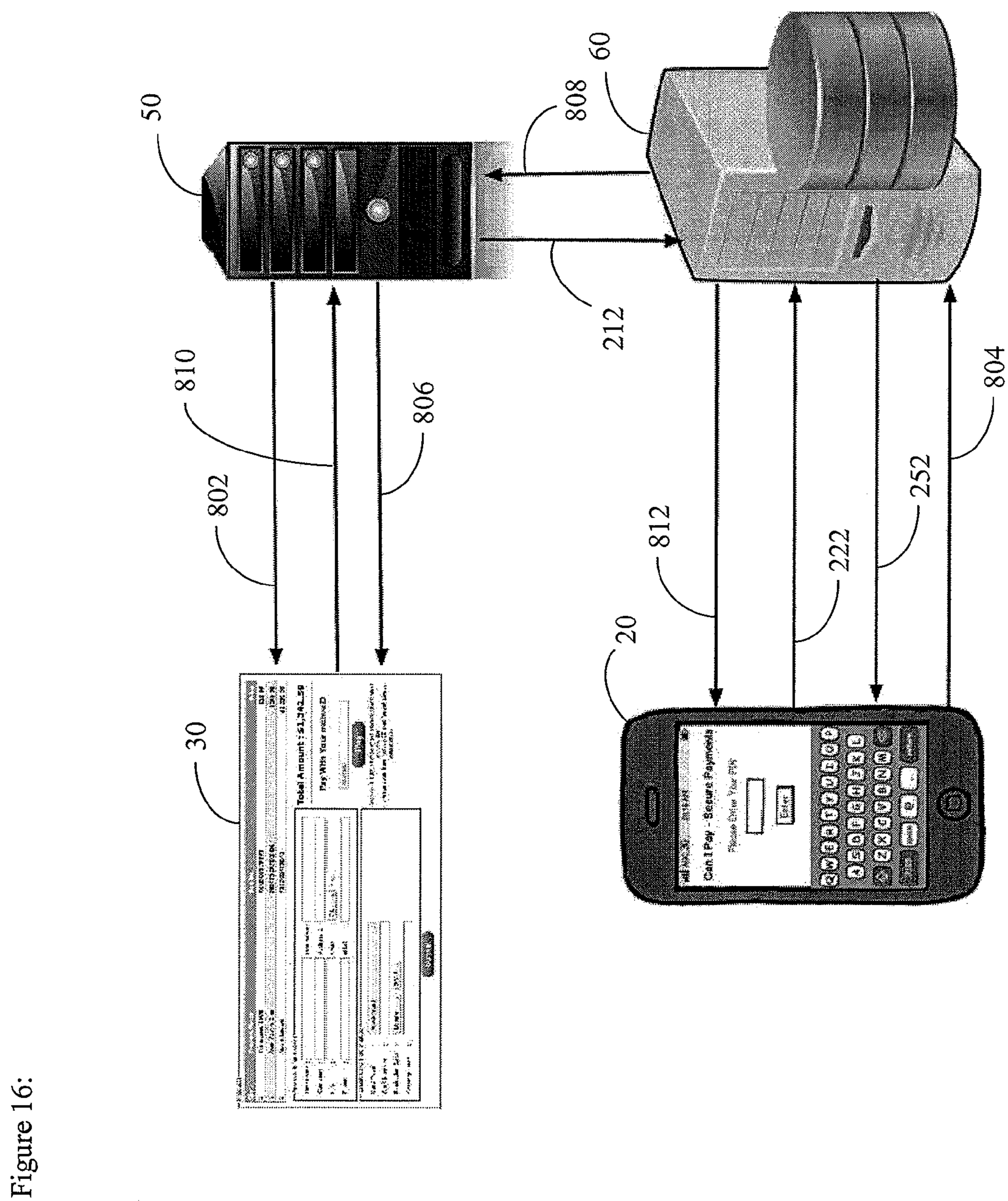


U.S. Patent

Mar. 18, 2014

Sheet 17 of 22

US 8,677,116 B1



U.S. Patent

Mar. 18, 2014

Sheet 18 of 22

US 8,677,116 B1

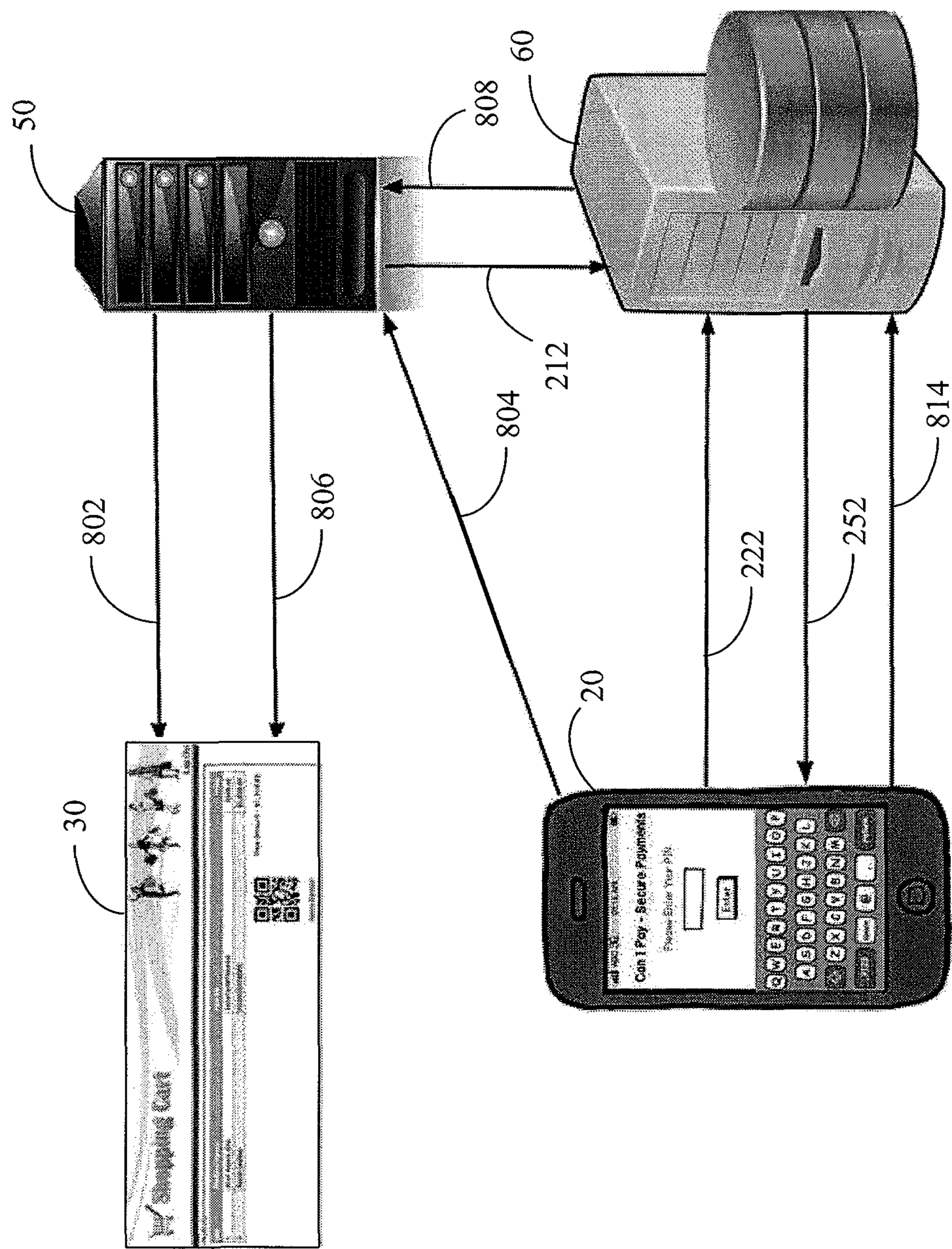


Figure 17:

U.S. Patent

Mar. 18, 2014

Sheet 19 of 22

US 8,677,116 B1

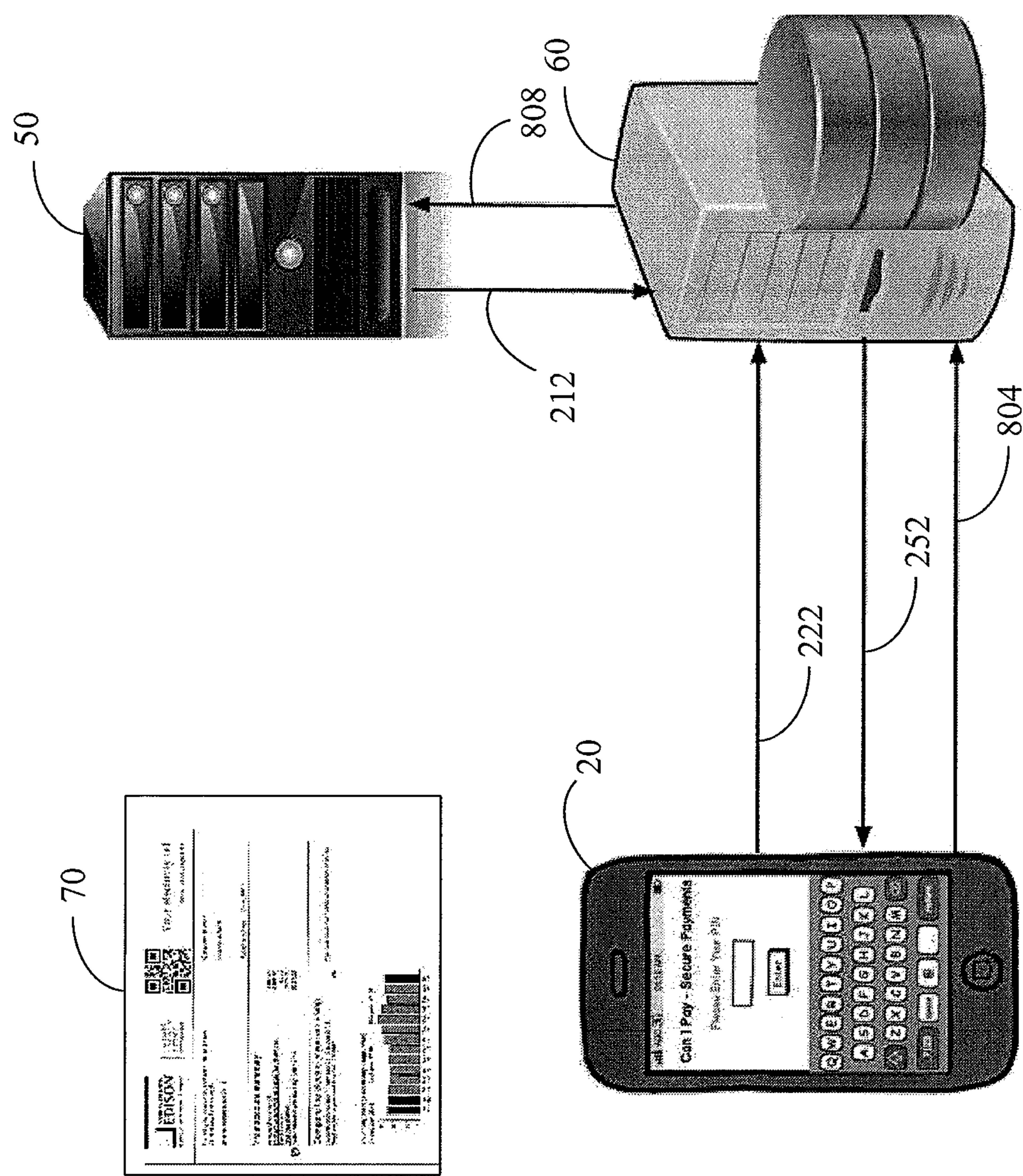


Figure 18:

U.S. Patent

Mar. 18, 2014

Sheet 20 of 22

US 8,677,116 B1

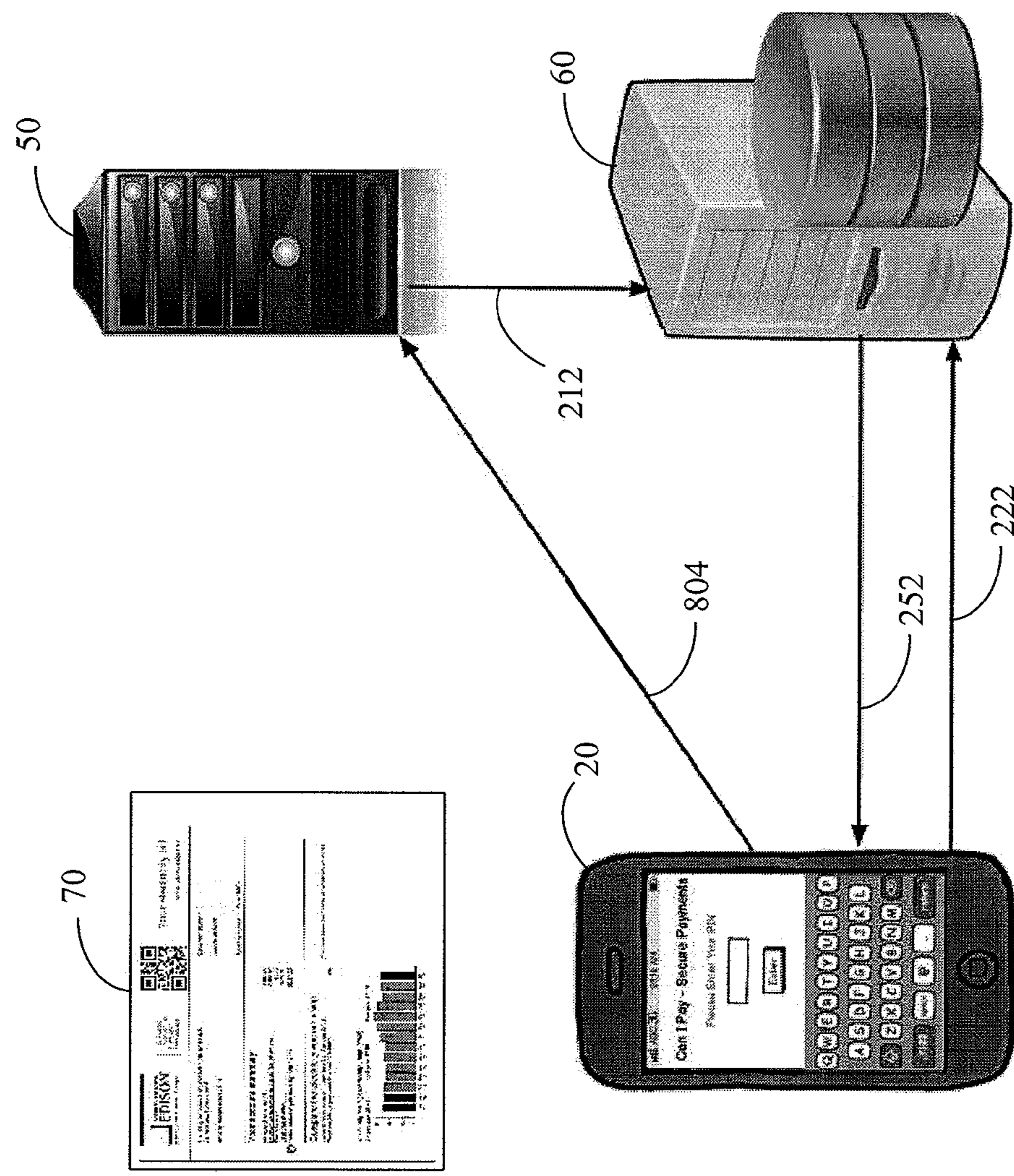


Figure 19:

U.S. Patent

Mar. 18, 2014

Sheet 21 of 22

US 8,677,116 B1

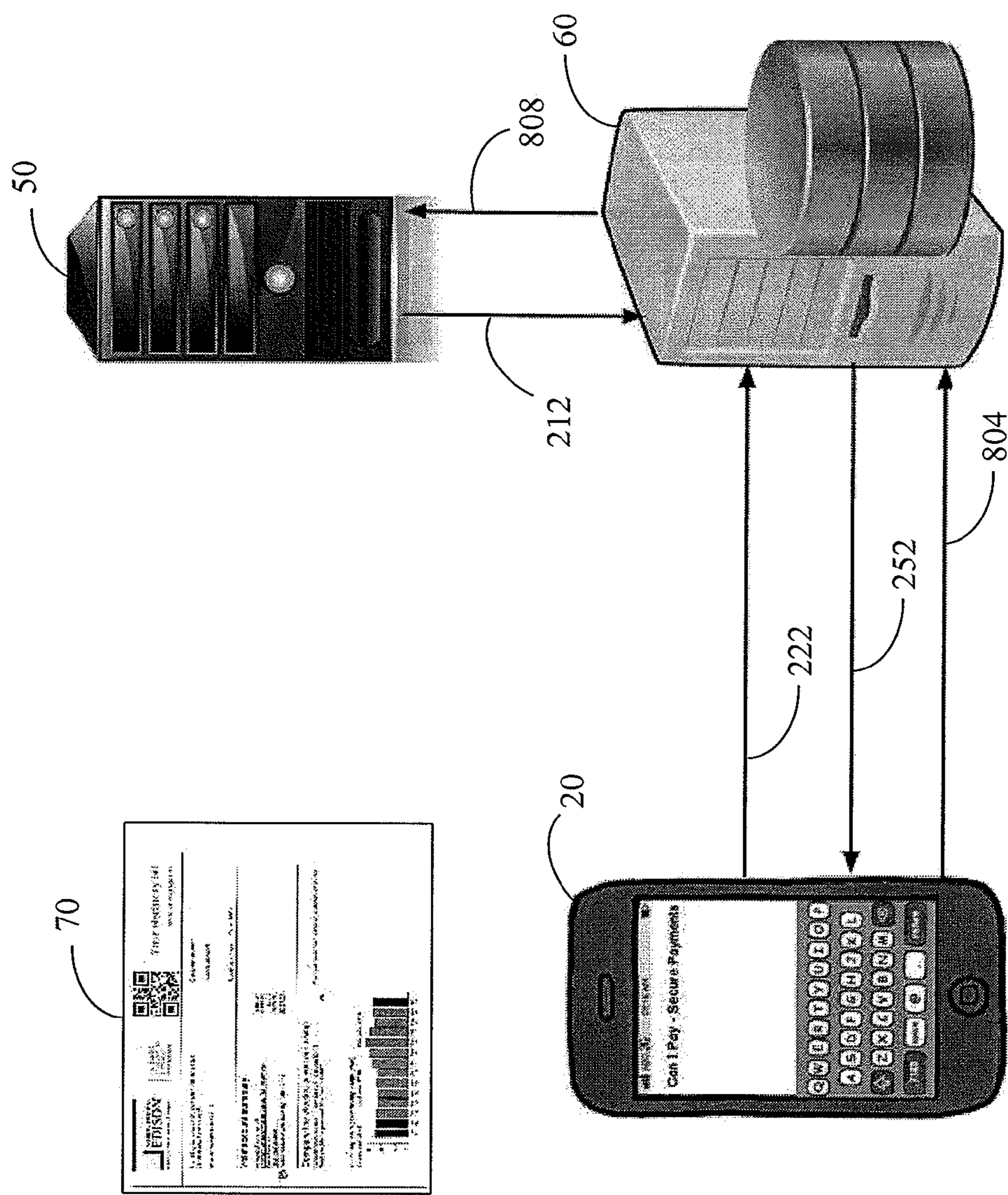


Figure 20:

U.S. Patent

Mar. 18, 2014

Sheet 22 of 22

US 8,677,116 B1

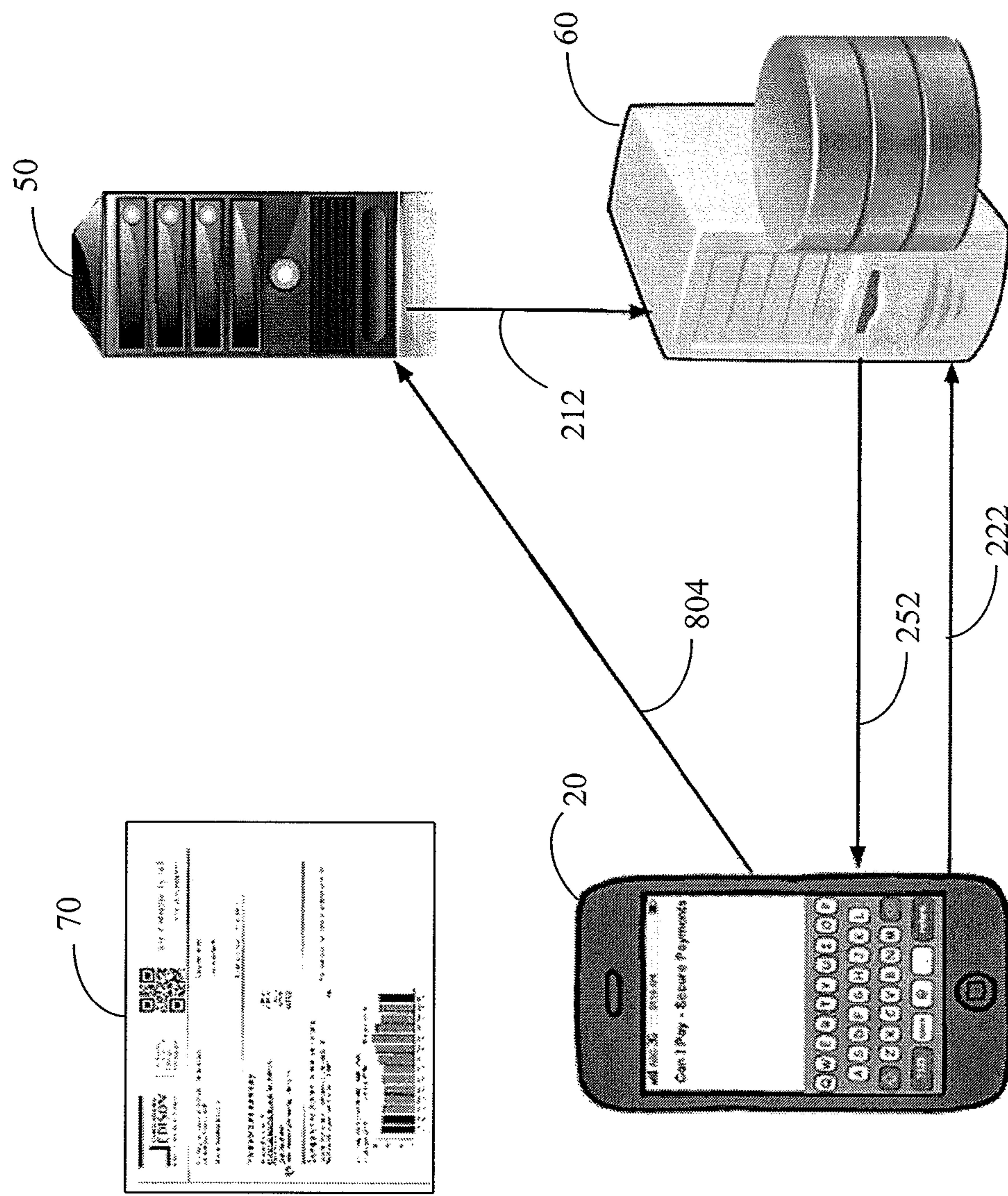


Figure 21:

## US 8,677,116 B1

**1****SYSTEMS AND METHODS FOR AUTHENTICATION AND VERIFICATION****CROSS-REFERENCE TO RELATED APPLICATIONS**

This application claims the benefit of priority to U.S. Provisional Appl. No. 61/729,266, filed Nov. 21, 2012 and U.S. Provisional Appl. No. 61/772,110, filed Mar. 4, 2013, both of which are incorporated in their entirety by reference herein.

**BACKGROUND****1. Field**

This application is generally directed to systems and methods for authentication and verification of users, and more specifically to such systems and methods utilizing a mobile or portable device.

**2. Description of the Related Art**

There is a growing need to authenticate users trying to access a secured internet portal (e.g., website) or a real-world secured device (e.g., lock, door) that can be actuated via the internet. In addition, with more and more consumer transactions occurring over the internet, the need for a secure and fast online electronic payment capability is also growing.

**SUMMARY**

In certain embodiments, a method is provided for authenticating a user seeking to conduct at least one interaction with a secured capability provided by a computer. The method comprises receiving a first signal from the computer providing the secured capability. The first signal comprises a reusable identifier corresponding to the secured capability. The method further comprises receiving a second signal from an electronic device being used by the user. The second signal comprises a copy of the reusable identifier and user verification information. The method further comprises using a processor to evaluate, based at least on the first signal and the second signal, whether the user is authorized to conduct the at least one interaction with the secured capability. The method further comprises, in response to an indication from the processor that the user is authorized to conduct the at least one interaction with the secured capability, transmitting a third signal comprising authorization information to at least one of the electronic device and the computer. In certain embodiments, a non-transitory (e.g., tangible) computer storage is provided having stored thereon a computer program (e.g., code) that instructs a computer system to perform the method described in this paragraph.

In certain embodiments, a computer system is provided for authenticating users seeking to conduct interactions with a plurality of secured capabilities. The computer system comprises a first input configured to receive a plurality of first signals from a plurality of computers. Each computer of the plurality of computers provides at least one secured capability of the plurality of secured capabilities. Each first signal of the plurality of first signals comprises a reusable identifier corresponding to a secured capability of the plurality of secured capabilities. The computer system further comprises a second input configured to receive a plurality of second signals from a plurality of electronic devices being used by the users. Each second signal of the plurality of second signals comprises a copy of a reusable identifier and user verification information. The computer system further comprises a storage device comprising a first association of each secured capability of the plurality of secured capabilities with at least

**2**

one corresponding reusable identifier, and a second association of the user verification information with corresponding verified users authorized to access at least one secured capability of the plurality of secured capabilities. The computer system further comprises a processor configured to evaluate, based at least on a first signal received from a computer of the plurality of computers and a second signal received from an electronic device of the plurality of electronic devices, whether a user of the electronic device is authorized to conduct at least one interaction with a secured capability corresponding to the reusable identifier. The computer system further comprises an output configured to transmit a third signal comprising authorization information to at least one of the electronic device and the computer providing the secured capability corresponding to the reusable identifier, if the user of the electronic device is authorized to conduct the at least one interaction with the secured capability corresponding to the reusable identifier.

In certain embodiments, a method is provided for authenticating users seeking to conduct at least one interaction with a secured capability. The method comprises transmitting a first signal to a verification server. The first signal comprises a reusable identifier corresponding to the secured capability. The verification server is configured to receive validation data from an electronic device being used by the user and is further configured to evaluate, based at least on the validation data and the reusable identifier, whether the user is authorized to conduct the at least one interaction with the secured capability. The method further comprises transmitting a second signal to the user. The second signal comprises the reusable identifier. The method further comprises receiving authorization information from at least one of the verification server and the electronic device. The method further comprises using a processor to provide the user with access to conduct the at least one interaction with the secured capability in response at least to the authorization information. In certain embodiments, a non-transitory (e.g., tangible) computer storage is provided having stored thereon a computer program (e.g., code) that instructs a computer system to perform the method described in this paragraph.

In certain embodiments, a method is provided for authenticating users seeking to conduct at least one interaction with a secured capability. The method comprises storing a plurality of identifiers corresponding to the secured capability. The method further comprises selecting a first identifier of the plurality of identifiers to be presented to a first user and to a verification server to initiate a first interaction with the first user. The first identifier is to be presented to the first user in a first form configured to be detected by a first electronic device being used by the first user. The verification server is configured to receive the plurality of identifiers and to receive validation signals from electronic devices being used by the users. The verification server is further configured to evaluate, based at least on the received validation signals and identifiers, whether the users are authorized to conduct the at least one interaction with the secured capability. The method further comprises selecting a second identifier of the plurality of identifiers to be presented to a second user and to the verification server to initiate a second interaction with the second user. The second identifier is to be presented to the second user in a second form configured to be detected by a second electronic device being used by the second user. The method further comprises selecting the first identifier to be presented to a third user and to the verification server to initiate a third interaction with the third user. The first identifier is to be presented to the third user in a third form configured to be detected by a third electronic device being used by the third

## US 8,677,116 B1

**3**

user. In certain embodiments, a non-transitory (e.g., tangible) computer storage is provided having stored thereon a computer program (e.g., code) that instructs a computer system to perform the method described in this paragraph.

In certain embodiments, a method is provided for authenticating a user seeking to conduct at least one interaction with a secured capability provided by a computer. The method comprises detecting an encoded identifier comprising a reusable identifier corresponding to the secured capability. The method further comprises using a processor to decode the encoded identifier to extract the reusable identifier. The method further comprises transmitting validation data to a validation server. The validation data comprises the extracted reusable identifier and a user verification code. The verification server is configured to evaluate, based at least on the validation data and the reusable identifier, whether the user is authorized to access the secured capability. In certain embodiments, a non-transitory (e.g., tangible) computer storage is provided having stored thereon a computer program (e.g., code) that instructs a computer system to perform the method described in this paragraph.

The paragraphs above recite various features and configurations of one or more methods, computer systems, and computer storage, that have been contemplated by the inventor. It is to be understood that the inventor has also contemplated methods, computer systems, and computer storage which comprise combinations of these features and configurations from the above paragraphs, as well as methods, computer systems, and computer storage which comprise combinations of these features and configurations from the above paragraphs with other features and configurations disclosed in the following paragraphs.

## BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 schematically illustrates an example configuration in which certain embodiments described herein can be used.

FIG. 2 schematically illustrates an example subset of the configuration of FIG. 1 showing an aspect of communication among components of the configuration in accordance with certain embodiments described herein.

FIG. 3A is a flow diagram of an example method of authenticating a user seeking to conduct at least one interaction with a secured capability provided by a computer, in accordance with certain embodiments described herein.

FIG. 3B schematically illustrates an example computer system (e.g., a verification server) in accordance with certain embodiments described herein.

FIG. 4 is a flow diagram of an example method of authenticating users seeking to conduct at least one interaction (e.g., retrieval of information from a secured internet portal, a purchase, opening a lock selectively inhibiting physical entry to an enclosed region within a safe, building, or vehicle) with a secured capability in accordance with certain embodiments described herein.

FIG. 5 is a flow diagram of an example method of authenticating users seeking to conduct at least one interaction with a secured capability in accordance with certain embodiments described herein.

FIG. 6 is a flow diagram of an example method of authenticating users seeking to conduct at least one interaction with a secured capability in accordance with certain embodiments described herein.

FIG. 7 schematically illustrates a first example configuration for providing a secured authentication/login in accordance with certain embodiments described herein.

**4**

FIG. 8 schematically illustrates a second example configuration for providing a secured authentication/login in accordance with certain embodiments described herein.

FIG. 9 schematically illustrates a third example configuration for providing a secured authentication/login in accordance with certain embodiments described herein.

FIG. 10 schematically illustrates a fourth example configuration for providing a secured authentication/login in accordance with certain embodiments described herein.

FIG. 11 schematically illustrates a fifth example configuration for providing a secured authentication/login in accordance with certain embodiments described herein.

FIG. 12 schematically illustrates a sixth example configuration for providing a secured authentication/login in accordance with certain embodiments described herein.

FIG. 13 schematically illustrates a first example configuration for providing a secured electronic payment capability in accordance with certain embodiments described herein.

FIG. 14 schematically illustrates a second example configuration for providing a secured electronic payment capability in accordance with certain embodiments described herein.

FIG. 15 schematically illustrates a third example configuration for providing a secured electronic payment capability in accordance with certain embodiments described herein.

FIG. 16 schematically illustrates a fourth example configuration for providing a secured electronic payment capability in accordance with certain embodiments described herein.

FIG. 17 schematically illustrates a fifth example configuration for providing a secured electronic payment capability in accordance with certain embodiments described herein.

FIG. 18 schematically illustrates a sixth example configuration for providing a secured electronic payment capability in accordance with certain embodiments described herein.

FIG. 19 schematically illustrates a seventh example configuration for providing a secured electronic payment capability in accordance with certain embodiments described herein.

FIG. 20 schematically illustrates an eighth example configuration for providing a secured electronic payment capability in accordance with certain embodiments described herein.

FIG. 21 schematically illustrates a nineteenth example configuration for providing a secured electronic payment capability in accordance with certain embodiments described herein.

## DETAILED DESCRIPTION

While various embodiments are described herein by citing websites and smartphones as examples of devices which can be used, the systems and methods described herein are not so limited. Certain embodiments also extend to bank safes, door locks, and any other objects that use some form of security to access, and other forms of mobile personal devices (e.g., electronic tablets). Certain embodiments described herein can be used to provide higher security to access any secured or sensitive information or object. For example, certain embodiments can be used to allow users be identified and verified as being among those individuals who are authorized to access information that is secured or that is sensitive.

Although commonly used terms are used to describe the systems and methods of certain embodiments for ease of understanding, these terms are used herein to have their broadest reasonable interpretation, as described in more detail herein.

## US 8,677,116 B1

5

FIG. 1 schematically illustrates an example configuration in which certain embodiments described herein can be used. A plurality of users **10** (e.g., user 1, user 2, . . . , user N) are each utilizing a first electronic device **20** (e.g., device 1a, device 2a, . . . , device Na) operatively coupled to a network **40** (e.g., the internet), and a second electronic device **30** (e.g., device 1b, device 2b, . . . , device Nb) operatively coupled to the network **40**. For example, the first electronic device **20** can be a personal computer (e.g., laptop, notebook) that is running a web browser program (e.g., Internet Explorer®, Firefox®, Safari®) to access or visit websites hosted by one or more computers **50** (e.g., computer 1, computer 2, computer 3, . . . , computer M) via the network **40**, or can be a mobile device (e.g., smartphone or tablet) that is running an application that accesses or visits websites hosted by the one or more computers **50** via the network **40**, and the second electronic device **30** can be a mobile device (e.g., smartphone or tablet) that is running an application that accesses the network **40**. The computers **50** (e.g., web servers) can each provide at least one secured capability (e.g., access to secured information, access to conduct a secure transaction) with which authorized users visiting the website are to conduct at least one interaction.

A verification server **60** (e.g., a computing device that can authorize a connection or a validation attempt) is also operatively coupled to the network **40** as is described more fully herein. While FIG. 1 shows an example configuration in which the verification server **60** is separate from the one or more computers **50** (e.g., as a specific server operatively coupled to the network), in other example configurations, the verification server **60** is integrated with one or more of the computers **50**. In certain embodiments, two or more verification servers **60** may be used.

Certain embodiments described herein include methods which are performed by computer hardware, software or both, comprising one or more modules. The hardware used for certain embodiments described herein (e.g., the first electronic devices **20**, the second electronic devices **30**, the computers **50**, and the validation server **60**) can take a wide variety of forms, including processors, general-purpose computers, network servers, workstations, personal computers, mainframe computers and the like. The hardware running the software will typically include one or more input devices, such as a mouse, trackball, touchpad, and/or keyboard, a display, and computer-readable memory media, such as random-access memory (RAM) integrated circuits and a data storage device (e.g., tangible storage, non-transitory storage, flash memory, hard-disk drive). It will be appreciated that one or more portions, or all of the software code may be remote from the user and, for example, resident on a network resource, such as a LAN server, Internet server, network storage device, etc. The software code which configures the hardware to perform in accordance with certain embodiments described herein can be downloaded from a network server which is part of a local-area network or a wide-area network (such as the internet) or can be provided on a tangible (e.g., non-transitory) computer-readable medium, such as a CD-ROM or a flash drive. Various computer languages, architectures, and configurations can be used to practice the various embodiments described herein.

FIG. 2 schematically illustrates an example subset of the configuration of FIG. 1 showing an aspect of communication among components of the configuration in accordance with certain embodiments described herein. In the example communication scheme of FIG. 2, the user **10** utilizes a first electronic device **20** as described below in an authorization (e.g., authentication, verification) process. While the descrip-

6

tion herein includes numerous communication schemes, the example communication scheme of FIG. 2 can be helpful for understanding the general context in which certain embodiments described herein can be used. In the example configuration of FIG. 2, a user **10** can use the second electronic device **30** (e.g., a computer with a user browser running a browser window viewed on a display device) to view content provided by the computer **50** (e.g., web server) with the intention of conducting an interaction with a secured capability of the computer, such as entering into a secure environment or website (e.g., to access secure information or sensitive information) or making a payment as part of an ecommerce transaction. The computer **50** of the example configuration of FIG. 2 provides a reusable identifier both to the second electronic device **30** (e.g., with the reusable identifier encoded as a QR code) and to the verification server **60** (e.g., a computing device that can authorize an interaction) with the reusable identifier serving as a start signal for the authentication process. Using the first electronic device **20** (e.g., a mobile device, such as a smartphone), the user **10** can scan the QR code displayed by the second electronic device **30** and can extract the reusable identifier from the displayed QR code. The first electronic device **20** then transmits the extracted reusable identifier and user verification information to the verification server **60**. In response at least to the reusable identifier received from the first computer **50**, the reusable identifier received from the first electronic device **20**, and the user verification information received from the first electronic device **20**, the verification server **60** determines whether the user **10** is authorized to conduct the interaction with the secured capability. If the user is authorized, the verification server **60** can send an authorization signal to the computer **50**, which then provides the access to the user **10**.

In certain embodiments described herein, using the reusable identifier provides advantages not available from conventional systems. For example, by using reusable identifiers that do not include user-specific or transaction-specific information, details regarding the transaction (e.g., items to be purchased, pricing, user information, shipping information) can be updated or changed without having to produce a new identifier. For another example, by not including user-specific or transaction-specific information in the reusable identifier, the QR code in which the reusable identifier is encoded can be much simpler than in systems in which the QR code encodes additional information. Thus, the QR code can have larger light and dark regions in a given image (e.g., less resolution is needed to read the QR code), making the QR code more easily read and decoded (e.g., using the limited computing power and optical resolution of many mobile devices) and the process is faster and more reliable, thereby contributing to a favorable user experience, which can be a key to market acceptance. For another example, such QR codes would not require real-time instantaneous generation of complex graphical images (the QR codes), thereby reducing server computing requirements and increasing server scalability to serve a higher number of users and processing a higher number of transactions as compared to one-time-use QR codes. For another example, since no user- or transaction-specific information is contained in the reusable identifiers, such identifiers are safer to use, and do not require complex and time-consuming encryption/decryption processes to protect sensitive data.

FIG. 3A is a flow diagram of an example method **100** of authenticating a user **10** seeking to conduct at least one interaction with a secured capability provided by a computer **50**, in accordance with certain embodiments described herein. FIG. 3B schematically illustrates an example computer system **200**

## US 8,677,116 B1

7

(e.g., a verification server 60) in accordance with certain embodiments described herein for performing the method 100. The example method 100 is described herein with regard to the aspects of an authorization process that are performed by a computer system 200 (e.g., a verification server 60). Other methods are described herein with regard to the aspects of an authorization process that are performed by the computer 50 and to the aspects of an authorization process that are performed by the electronic device 20. While the method 100 is described below by referencing the structural components shown in FIG. 3B, the method 100 may be performed by other structural components.

In an operational block 110, the method 100 comprises receiving a first signal 212 from the computer 50 providing the secured capability. The first signal 212 comprises a reusable identifier 214 corresponding to the secured capability. In an operational block 120, the method 100 further comprises receiving a second signal 222 from an electronic device 20 being used by the user 10. The second signal 222 comprises the first reusable identifier 214 (e.g., a copy 224 of the reusable identifier 214 of the first signal 212) and user verification information 226. In an operational block 130, the method 100 further comprises using a processor 240 to evaluate, based at least on the first signal 212 and the second signal 222, whether the user 10 is authorized to conduct the at least one interaction with the secured capability. In an operational block 140, the method 100 further comprises transmitting, in response to an indication from the processor 240 that the user 10 is authorized to conduct the at least one interaction with the secured capability, a third signal 252 comprising authorization information 254 to at least one of the electronic device 20 and the computer 50.

The computer system 200 (e.g., a verification server 60) comprises a first input 210 configured to receive a plurality of first signals 212 from a plurality of computers 50. Each computer 50 of the plurality of computers 50 is configured to provide at least one secured capability of the plurality of secured capabilities. Each first signal 212 of the plurality of first signals 212 comprises a reusable identifier 214 corresponding to a secured capability of the plurality of secured capabilities. The computer system 200 further comprises a second input 220 configured to receive a plurality of second signals 222 from a plurality of electronic devices 20 being used by the users 10. Each second signal 222 of the plurality of second signals 222 comprises a reusable identifier 214 (e.g., a copy 224 of a reusable identifier 214 of a first signal 212) and user verification information 226. The computer system 200 further comprises a storage device 230 comprising a first association 232 of each secured capability of the plurality of secured capabilities with at least one corresponding reusable identifier 214. The storage device 230 further comprises a second association 234 of the user verification information 226 with corresponding verified users 10 authorized to access at least one secured capability of the plurality of secured capabilities. The computer system 200 further comprises a processor 240 configured to evaluate, based at least on a first signal 212 received from a computer 50 of the plurality of computers 50 and a second signal 222 received from an electronic device 20 of the plurality of electronic devices 20, whether a user 10 of the electronic device 20 is authorized to conduct at least one interaction with a secured capability corresponding to the reusable identifier 214. The computer system 200 further comprises an output 250 configured to transmit a third signal 252 comprising authorization information 254 to at least one of the electronic device 20 and the computer 50 providing the secured capability corresponding to the reusable identifier 214, if the user 10 of the

8

electronic device 20 is authorized to conduct the at least one interaction with the secured capability corresponding to the reusable identifier 214.

The first input 210, the second input 220, and the output 250 are each configured to be operationally coupled to the network 40 (e.g., the internet). In certain embodiments, two or more of the first input 210, the second input 220, and the output 250 can be integrated together in a network portal, or can be distributed among one, two, or more network portals. The first input 210, the second input 220, and the output 250 are also configured to communicate with one or both of the storage device 230 and the processor 240 of the computer system 200.

In certain embodiments, the verification server 60 is configured to remotely disable the ability to use the electronic device 20 in an authorization process. For example, a separate website or push message may be used to communicate to the verification server 60 that the security of the electronic device 20 has been compromised (e.g., the electronic device 20 has been stolen), so communications with the electronic device 20 should no longer be used. In certain embodiments, information or data relevant to the authorization process can be remotely deleted from the electronic device 20 (e.g., via a push message) in the event that the security of the electronic device 20 has been compromised.

In certain embodiments, the secured capability can comprise a structure (e.g., a locked door, fence, gate, elevator) that is operatively coupled to the computer 50 and that is configured to selectively inhibit physical access to a region (e.g., interior of a safe, building, house, vehicle, automobile) or operation of a machine (e.g., automobile, elevator) to only authorized users, and the at least one interaction can comprise access to the restricted region (e.g., opening a lock thereby allowing entry to or exit from the restricted region) or turning the machine on or off. In certain embodiments, the secured capability can comprise a security module that is run by or operatively coupled to the computer 50 and that is configured to selectively restrict access to a memory region (e.g., a database, a secured internet portal) to only authorized users, and the at least one interaction can comprise access to the restricted memory region (e.g., retrieval of information from the secured internet portal, writing to or reading from the restricted memory region). In certain embodiments, the secured capability can comprise an electronic payment module that is run by or operatively coupled to the computer 50 and that is configured to selectively restrict access to an electronic payment as part of an ecommerce transaction (e.g., purchase) with the user that initiated the transaction, and the at least one interaction can comprise a transfer of funds (e.g., from the user to a merchant) to conduct the ecommerce transaction.

In certain embodiments, the reusable identifier 214 corresponds to a particular secured capability and serves as a “transaction start indicator” or “TSSID” that denotes the beginning of a process. The reusable identifier 214 may include data, such as information about the company providing the secured capability, the particular secured capability that corresponds to the TSSID, or both. For example, the reusable identifier 214 can include a short sequence of numbers, letters, or characters that identifies the company providing the secured capability, the secured capability, or both. In certain embodiments having two or more verification servers 60, the reusable identifier 214 can comprise information identifying which of the verification servers 60 is to be used. In certain embodiments, the reusable identifier 214 does not contain information about the company providing the secured capability. In certain embodiments, the reusable identifier

## US 8,677,116 B1

9

**214** includes only numbers, not alphabetic characters, which can make the visual identifier (e.g., QR code) which encodes the reusable identifier **214** more simple and easier to scan. In certain embodiments, the reusable identifier **214** does not comprise data that is to be kept confidential, so the data of the reusable identifier **214** may or may not be encrypted.

As used herein, the term “reusable” in conjunction with the reusable identifier **214** has its broadest reasonable interpretation, including but not limited to, an identifier that can be used more than once (e.g., the identifier is not for merely “one-time-use,” is not unique to one particular user or transaction, or both). For example, a reusable identifier **214** (e.g., a reusable TSSID) signals the beginning of a transaction, does not contain user-specific or transaction-specific information, and can be reused for multiple users and multiple transactions. In certain embodiments described herein, a reusable identifier **214** is utilized in a different way than the “one-time-use” or “unique” identifiers (IDs) of conventional systems (e.g., systems that utilize identifiers containing transaction-specific information, so that, for example, when a smartphone sends login or payment information to a webserver, the webserver can associate the user to the transaction).

In certain embodiments, a predefined and previously generated list of the reusable identifiers **214** can be assigned to each secured capability of each computer **50**. The reusable identifier **214** assigned to each secured capability can be stored in the storage device **230** in the first association **232** (e.g., a database or look-up table) that keeps track of both the reusable identifiers **214** and the secured capabilities to which they are assigned. The reusable identifiers **214** to be used by a computer **50** can also be stored in a storage device of the computer **50**. The individual reusable identifiers **214** assigned to a secured capability can be used by the computer **50** sequentially (e.g., one after another, for sequential attempts to authenticate users seeking to conduct at least one interaction with the secured capability). In certain such embodiments, when all the reusable identifiers **214** of the predefined and previously generated list for the secured capability have been used by the computer **50** to denote various users seeking to access the secured capability, the computer **50** can go back and restart the list by again using the reusable identifiers **214** on the list (round robin usage). In certain embodiments, the reusable identifiers **214** are each only valid for a finite and predetermined period of time (e.g., one or more minutes, one or more hours, one or more days) but can be used in multiple such periods of time. For example, in certain embodiments, while the same reusable identifier **214** cannot be used again within the same time period, the reusable identifier **214** can be reused in a subsequent period of time (e.g., after one or more other reusable identifiers **214** have been selected and used sequentially in a round robin fashion). For another example, in certain embodiments, once a new time period is started, one or more previously-used reusable identifiers **214** can be used, even if the list of reusable identifiers **214** has not yet been exhausted within the previous time period (e.g., the round-robin processing does not have to be continued). Certain such embodiments are different from systems which utilize “one-time-use” TSSIDs or IDs.

In certain embodiments, the user **10** utilizes a second electronic device **30** to conduct the at least one interaction with the secured capability provided by the computer **50**. For example, the second electronic device **30** can comprise a computer with a user browser running a browser window viewed on a display device or a mobile device (e.g., smartphone or tablet) running an application. In certain other embodiments, examples of which are described herein, the user **10** conducts the at least one interaction with the secured

10

capability provided by the computer **50** without using a second electronic device **30**. For example, the reusable identifier **214** can be encoded in a QR code on a printed sheet of paper **70** (e.g., a bill or invoice).

In certain embodiments, the reusable identifier **214** is displayed or presented in a manner in which the electronic device **20** is able to receive the reusable identifier **214** from the second electronic device **30**. For example, the reusable identifier **214** can be presented (e.g., by the second electronic device **30** which received the reusable identifier **214** from the computer **50**) as an reusable encoded visual or auditory identifier configured to be detected by the electronic device **20** and decoded by a program executed by the electronic device **20** to yield the reusable identifier **214**. The visual or auditory identifiers can be predetermined (e.g., premade) based on the predetermined reusable identifiers **214**, or each visual or auditory identifiers can be generated just before it is to be presented to and detected by the electronic device **20**. Since they encode the reusable identifiers **214**, the visual or auditory identifiers can also be reusable (e.g., used more than once and not for merely “one-time-use,” not unique to one particular user or transaction, or both). In certain embodiments, the visual or auditory identifiers are each only valid for a finite and predetermined period of time (e.g., one or more minutes, one or more hours, one or more days) but can be used in multiple such periods of time. The visual or auditory identifiers can be stored in the verification server **60** (e.g., the storage device **230**) and provided to the computer **50** as needed, or the visual or auditory identifiers can be stored on the computer **50** (e.g., a web server) to be used as needed. In certain embodiments, the visual or auditory identifiers are used sequentially, in a round robin fashion.

In certain embodiments, the visual or auditory identifier comprises visual signals (e.g., static images, color images, black and white images, striped images, flashing lights, animated images, videos) or auditory signals (e.g., tones, sounds, music) containing the reusable identifier **214** and that are decoded by a program executed by the first electronic device **20**. For example, a visual identifier can be presented on a visual display device of the second electronic device **30** (e.g., by a user browser or on a printed page) and detected by a camera or light sensor of the first electronic device **20**. For another example, an auditory identifier can be presented by a speaker of the second electronic device **30** and detected by a microphone of the first electronic device **20**. In certain embodiments, instead of, or in conjunction with, the visual or auditory identifier, a radio signal can be used to encode the reusable identifier **214** with the electronic device **20** configured to receive and decode the radio signal.

In certain embodiments, the visual or auditory identifier comprises a QR code, which is a graphical static image that can be used to encode information and that can be detected by a camera and decoded by software. For example, a QR code containing the reusable identifier **214** can be presented (e.g., by the second electronic device **30** or on a printed page) and can be detected by the electronic device **20** (e.g., smartphone or tablet) and decoded by a program executed by the electronic device **20** to yield the reusable identifier **214**. The QR code can be predetermined (e.g., premade) based on the predetermined reusable identifiers **214**, or each QR code can be generated just before it is to be presented to and detected by the electronic device **20**. Since they encode the reusable identifiers **214**, the QR codes can also be reusable (e.g., used more than once and not for merely “one-time-use,” not unique to one particular user or transaction, or both). In certain embodiments, the QR codes are each only valid for a finite and predetermined period of time (e.g., one or more minutes, one

## US 8,677,116 B1

**11**

or more hours, one or more days) but can be used in multiple such periods of time. The QR codes can be stored in the verification server **60** (e.g., the storage device **230**) and provided to the computer **50** as needed, or the QR codes can be stored on the computer **50** (e.g., a web server) to be used as needed. In certain embodiments, the QR codes are used sequentially, in a round robin fashion.

In certain embodiments, the first electronic device **20** comprises a device, such as a smartphone or a tablet, capable of detecting the visual or auditory identifier (e.g., QR Code) and communicating with the verification server **60** via a network or the internet. In certain embodiments, the second electronic device **30** comprises a display device (e.g., LED display, audio speaker, electric bulb or LED) capable of presenting the visual or auditory identifier (e.g., QR code) in a manner detectable by the first electronic device **20**. In certain such embodiments, the display device is running a user browser connected to the computer **50** via the internet. In certain embodiments, the computer **50** comprises a processor running a web server and driving the display device (e.g., by transmitting HTML information to the user browser of the display device). The computer **50** may be integrated with or separated from the display device of the second electronic device **30**. In certain embodiments, the verification server **60** comprises a processor configured to authorize a connection or a validation attempt by the user **10**. For example, verification server **60** can be integrated with or separated from the computer **50**. In certain embodiments described herein, the verification server **60** comprises one or more specific servers sitting on the internet and containing user verification information. In certain embodiments described herein, the first electronic device **20** comprises a mobile smartphone capable of scanning and decoding a QR code displayed by a user browser running on the second electronic device **30**, with the QR code encoding the reusable identifier **214**. The smartphone is also configured to communicate the decoded identifier, along with user verification information, to the verification server **60** via the network **40** (e.g., the internet).

In certain embodiments, the computer **50** transmits the first signal **212** to the verification server **60**, which receives the first signal **212** from the computer **50** in the operational block **110**. The first signal **212** comprises the reusable identifier **214** and can be interpreted by the verification server **60** as the initiation of an authentication process. In certain embodiments, the computer **50** also transmits the reusable identifier **214** to the second electronic device **30** to be presented (e.g., in a visual or auditory identifier, such as a QR code) in a form that can be detected and decoded by the first electronic device **20**. This transmission of the reusable identifier **214** to the second electronic device **30** can be concurrent or non-concurrent with the transmission of the first signal **212** to the verification server **60**. In certain other embodiments, the reusable identifier **214** is presented to the user **10** by a visual identifier in which the reusable identifier **214** is encoded and which is printed on a page **70** (e.g., a bill or invoice).

The user **10** can use the first electronic device **20** to detect and decode the identifier being presented by the second electronic device **30** so as to generate a copy **224** of the reusable identifier **214**, which should be the same as the reusable identifier **214** (e.g., both the reusable identifier **214** and the copy **224** do not contain user-specific or interaction-specific information). The first electronic device **20** transmits the second signal **222** to the verification server **60**, which receives the second signal **222** from the first electronic device **20** in the operational block **120**. The second signal **222** comprises the reusable identifier **214** and the user verification information **226**.

**12**

The user verification information **226** can be stored on, or can be otherwise accessible by, the first electronic device **20**. In certain embodiments, the user verification information **226** comprises information that can be used to verify and authenticate the user (e.g., a verifiable “fingerprint” of the user and mobile device). For example, the user verification information **226** can comprise information regarding (e.g., specific to) the user (e.g., the user's first name, family name, email address, phone number), information regarding (e.g., specific to) the first electronic device **20** (e.g., a device identification character string, hardware-specific information such as manufacturer or operating system of the first electronic device **20**), or both. In certain embodiments, the user verification information **226** can comprise information derivable from user-specific information (e.g., predetermined portions of the user-specific information that would not themselves contain private information) or information derivable from device-specific information (e.g., predetermined portions of the device-specific information that would not themselves contain private information). The user verification information **226** may or may not be encrypted.

The user verification information **226** corresponding to users that are authorized to access at least one secured capability can be stored in the storage device **230** in the second association **234** (e.g., in a database or look-up table) that keeps track of both the user verification information **226** and the authorized user which it denotes. In certain embodiments, the user verification information **226** is not made available to the computer **50**. In certain embodiments, the second association **234** also includes information regarding which secured capabilities each of the users denoted by user verification information **226** is authorized to access. Use of such user verification information **226** (e.g., user-specific information, device-related information, or both) can provide a desired level of security to ensure that the user **10** attempting to access the secured capability is an authorized user.

After having received the first signal **212** and the second signal **222**, the verification server **60** can evaluate (e.g., using the processor **240**), based at least on the first signal **212** and the second signal **222**, whether the user **10** is authorized to conduct the at least one interaction with the secured capability in the operational block **130**. For example, the verification server **60** can correlate the first signal **212** with the corresponding second signal **222** by comparing the reusable identifier **214** from the first signal **212** and the copy **224** from the second signal **222**. For a correlated first signal **212** and second signal **222**, the reusable identifier **214** and the copy **224** will match. The verification server **60** can also utilize the reusable identifier **214** with the first association **232** of each secured capability with at least one corresponding reusable identifier **214** to identify the secured capability that the user **10** is attempting to access. For example, using the received reusable identifier **214**, the validation server **60** can access the first association **232** to determine (e.g., look up) which secured capability (or computer **50**, or both) corresponds to the received reusable identifier **214**. The verification server **60** can also utilize the user verification information **226** and the second association **234** of the user verification information **226** with corresponding verified users **10** to evaluate, based at least on the user verification information **226**, whether the user **10** of the first electronic device **20** is one of the verified users of the secured capability. For example, using the user verification information **226**, the verification server **60** can access the second association **234** to determine (e.g., look up) which user corresponds to the user verification information **226**. If the user verification server **226** received from the electronic device **20** does not match any of the entries of the

## US 8,677,116 B1

13

second association 234, then the user is deemed to not be one of the verified users of the secured capability. Also, in certain embodiments in which the second association 234 also includes information regarding which secured capabilities the user denoted by the user verification information 226 is authorized to access, the verification server 60 can use the second association 234, the user verification information 226, and the reusable identifier 214 to determine (e.g., look up) whether the user is authorized to access the particular secured capability that the user is seeking to access. In certain embodiments, the verification server 60 also checks whether the first electronic device 20 (e.g., mobile device, smartphone, tablet) is deactivated. For example, upon receipt of a notification (e.g., from the user or from a third party authorized to provide such notifications), the verification server 60 can place the user's first electronic device 20 on a stored list of deactivated first electronic devices 20 that have been deactivated from use by the verification server 60. Such notifications can be provided to the verification server 60 upon discovery that the user's first electronic device 20 is lost or stolen. Deactivated first electronic devices 20 (e.g., those on the stored list of deactivated devices) would not be authorized by the verification server 60. Certain such embodiments can provide a way for a user to deactivate a lost or stolen first electronic device 20 and to stop access by people other than the user.

In certain embodiments in which the reusable identifier 214 is only valid for a finite and predetermined period of time, the validation server 60 can determine a first time of receipt of the first signal 212 and a second time of receipt of the second signal 222, and can compare the time differential between the first time and the second time. If the time differential is less than or equal to the finite and predetermined period of time for the reusable identifier 214, the validation server 60 can evaluate that the user 10 is authorized to conduct the at least one interaction with the secured capability corresponding to the reusable identifier 214. If the time differential is greater than the finite and predetermined period of time for the reusable identifier 214, the validation server 60 can evaluate that the user 10 is not authorized to access the secured capability. In certain other embodiments in which the reusable identifier 214 is only valid for a finite and predetermined period of time, after the period of time has elapsed, the verification server 60 deletes the record corresponding to the reusable identifier 214 so it can be reused again. Certain such embodiments avoid performing any timestamp comparison.

Upon evaluating that the user 10 is authorized to access the secured capability, the verification server 60 can transmit a third signal 252 comprising authorization information 254 to at least one of the first electronic device 20 and the computer 50, in the operational block 140. The authorization information 254 can comprise a flag indicating that the user 10 is authorized to conduct the at least one interaction with the secured capability, can comprise additional information regarding the conditions of the user 10 accessing the secured capability (e.g., number of interactions that are authorized, the type of interactions that are authorized), or both. For example, in certain embodiments, the authorization information 254 sent to the computer 50 in the third signal 252 can comprise an identifier that is unique to the user 10. The computer 50 can use this identifier to identify the user 10. For example, for a login to a secured account, the computer 50 can use this identifier to select which user's account to present to the browser running on the electronic device 30.

In certain embodiments in which the secured capability is a purchase of an ecommerce transaction and the third signal 252 comprising the authorization information 254 is trans-

14

mitted to the first electronic device 20, the first signal 212 from the computer 50 can further comprise invoice information corresponding to the purchase, and the third signal 252 can also comprise the invoice information. In certain other embodiments, the invoice information is sent to the first electronic device 20 from a second output of the validation server 60.

The first electronic device 20 can respond to the third signal 252 by transmitting payment information to at least one of the computer 50 and the validation server 60. For example, the payment information can comprise a confirmation (e.g., in a fourth signal) that a payment by the user 10 was made, and the output 250 can be configured to transmit the confirmation to the computer 50. In certain embodiments, the payment information further comprises shipping information and/or billing information. For example, the first electronic device 20 can transmit to the computer 50 shipping information for delivery corresponding to the purchase. In certain embodiments, the payment information comprises one or more of the following: user information (e.g., one or more of the user's name, mailing address, email address, phone number), means of payment information (e.g., one or more credit card, debit card, checking or savings account information, or other payment account information), which can be stored on the electronic device 20 or can be stored and accessible elsewhere on the internet (e.g., "in the cloud"), shipping information (e.g., one or more user information data records indicating the address to be used for shipping; the shipping information field can be empty where there is no need for a physical product shipment, and one shipping information can be shared among one or more payment information fields), billing information (e.g., one or more user information data records indicating the address to be used for billing; the billing information field can be empty where there is no need for billing, and one billing information can be shared among one or more payment information fields), userID (e.g., a registered combination of alphanumeric, special characters, or both that may be optionally followed by a password input, as a separate input field, composed of alphanumeric, special characters, or both), and authorized Login URL (e.g., a special url, composed of a site login url and an authorized user identification).

In certain embodiments, the first electronic device 20 can respond to the third signal 252 by transmitting payment information to a payment gateway (e.g., a computer system with a processor configured to receive such payment information and to facilitate the transfer of funds) via the internet or a network. Certain such embodiments in which the first electronic device 20 transmits payment information to the payment gateway can advantageously reduce credit card theft or fraud, can significantly increase user security, can make compliance with Payment Card Industry (PCI) data security standards easier and less costly, and/or to make anonymous payments in which the user's name or credit card information are not provided to the merchant of the goods or services being purchased.

FIG. 4 is a flow diagram of an example method 300 of authenticating users seeking to conduct at least one interaction (e.g., retrieval of information from a secured internet portal, a purchase, opening a lock selectively inhibiting physical entry to an enclosed region within a safe, building, or vehicle) with a secured capability in accordance with certain embodiments described herein. The example method 300 is described herein with regard to the aspects of an authorization process that are performed by a computer 50 (e.g., web server). The computer 50 (e.g., web server) can comprise a processor configured to perform the method 300. While the method 300 is described below by referencing certain struc-

## US 8,677,116 B1

15

tural components and signals, the method 300 may be performed using other structural components and signals.

In an operational block 310, the method 300 comprises transmitting a first signal to a verification server 60. The first signal comprises a reusable identifier 214 (e.g., not containing user-specific or interaction-specific information) corresponding to the secured capability. The verification server 60 is configured to receive validation data (e.g., user verification information 226) from an electronic device 20 (e.g., mobile device, smartphone, tablet) being used by the user and is further configured to evaluate, based at least on the validation data and the reusable identifier 214, whether the user is authorized to conduct the at least one interaction with the secured capability. In an operational block 320, the method 300 further comprises transmitting a second signal comprising the reusable identifier 214 to the user. In an operational block 330, the method 300 further comprises receiving authorization information 254 from at least one of the verification server 60 and the electronic device 20. In an operational block 340, the method 300 further comprises using a processor to provide the user with access to conduct the at least one interaction with the secured capability in response at least to the authorization information.

As described herein, in certain embodiments, transmitting the second signal to the user in the operational block 320 comprises transmitting the second signal to a second electronic device 30 being used by the user. For example, the second electronic device 30 can comprise a computer with a visual display, a speaker, or both, configured to present the reusable identifier 214 as an encoded visual or auditory identifier (e.g., a QR code) configured to be detected by the electronic device 20 and decoded by a program executed by the electronic device 20.

In certain embodiments in which the at least one interaction comprises a purchase, the first signal can further comprises invoice information corresponding to the purchase. The method 300 in certain such embodiments further comprises receiving (e.g., by the computer 50) a confirmation of a payment (e.g., whether successful or unsuccessful) or payment information corresponding to the purchase by the user.

As described more fully below, in certain embodiments, transmitting the second signal to the user in the operational block 320 comprises providing the user with a printed page 70 on which the reusable identifier 214 is displayed as a visual identifier. The visual identifier (e.g., QR code) can be configured to be detected by the electronic device 20 and decoded by a program executed by the electronic device 20.

FIG. 5 is a flow diagram of an example method 400 of authenticating users seeking to conduct at least one interaction with a secured capability in accordance with certain embodiments described herein. The example method 400 is described herein with regard to the aspects of an authorization process that are performed by an electronic device 20 (e.g., mobile device, smartphone, tablet). The electronic device 20 (e.g., mobile device, smartphone, tablet) can comprise a processor configured to perform the method 400. While the method 400 is described below by referencing certain structural components and signals, the method 400 may be performed using other structural components and signals.

In an operational block 410, the method 400 comprises detecting an encoded identifier comprising a reusable identifier 214 corresponding to the secured capability. In an operational block 420, the method 400 further comprises using a processor (e.g., of an electronic device 20 being used by the user, examples of which include but are not limited to a mobile device, a smartphone, and a tablet) to decode the encoded identifier to extract the reusable identifier 214. In an

16

operational block 430, the method 400 further comprises transmitting validation data (e.g., by the processor of the electronic device 20 being used by the user) to a validation server 60 configured to evaluate, based at least on the validation data and the reusable identifier 214, whether the user is authorized to access the secured capability. The validation data can comprise the extracted reusable identifier 214 and user verification information 226 (e.g., at least one of user-specific information and device-specific information).

As described herein, in certain embodiments, the encoded identifier is presented by a second electronic device 30 being used by the user. For example, the second electronic device 30 can comprise a computer with a visual display, a speaker, or both, configured to present the reusable identifier 214 as an encoded visual or auditory identifier (e.g., a QR code) configured to be detected by the electronic device 20 and decoded by a program executed by the electronic device 20. In certain such embodiments, detecting the encoded identifier in the operational block 410 can comprise using the electronic device 20 to detect the encoded identifier being presented by the second electronic device 30.

As described more fully below, in certain embodiments, the encoded identifier is presented on a printed page 70 (e.g., as a QR code) presented to the user, and detecting the encoded identifier in the operational block 410 comprises scanning the printed page 70 (e.g., using a camera of the electronic device 20). The visual identifier (e.g., QR code) can be configured to be detected by the electronic device 20 and decoded by a program executed by the electronic device 20.

FIG. 6 is a flow diagram of an example method 500 of authenticating users seeking to conduct at least one interaction with a secured capability in accordance with certain embodiments described herein. For example, the at least one interaction can comprise opening a lock selectively inhibiting physical entry to an enclosed region within a safe, building, or vehicle, retrieval of information from a secured internet portal, or transmission of information for completing a transaction with a secured internet portal. The example method 500 is described herein with regard to the aspects of an authorization process that are performed by a computer 50 (e.g., web server). The computer 50 (e.g., web server) can comprise a processor configured to perform the method 500. While the method 500 is described below by referencing certain structural components and signals, the method 500 may be performed using other structural components and signals.

In an operational block 510, the method 500 comprises storing a plurality of identifiers corresponding to the secured capability. In certain embodiments, each identifier of the plurality of identifiers does not contain user-specific or interaction-specific information. In an operational block 520, the method 500 further comprises selecting and transmitting a first identifier of the plurality of identifiers to a first user and to a verification server 60 to initiate a first interaction with the first user. The first identifier is configured to be presented in a first form to a first electronic device 20a being used by the first user. The verification server 60 is configured to receive the plurality of identifiers and to receive validation signals from electronic devices 20 being used by the users. The verification server 60 is further configured to evaluate, based at least on the received validation signals and identifiers, whether the users are authorized to conduct the at least one interaction with the secured capability. In an operational block 530, the method 500 further comprises selecting and transmitting a second identifier of the plurality of identifiers to a second user and to the verification server 60 to initiate a second interaction with the second user. The second identifier is configured to be presented in a second form to a second electronic device 20b

## US 8,677,116 B1

17

being used by the second user. In an operational block 530, the method 500 further comprises selecting and transmitting the first identifier to a third user and to the verification server 60 to initiate a third interaction with the third user. The first identifier is configured to be presented in a third form to a third electronic device 20c being used by the third user.

In certain embodiments, at least one of the first form, the second form, and the third form comprises an encoded visual form (e.g., QR code) configured to be presented using a computer display, while in certain other embodiments, at least one of the first form, the second form, and the third form comprises an encoded auditory form configured to be presented using a computer speaker. At least one of the first form, the second form, and the third form can comprise an encoded visual form (e.g., QR code) on a printed page 70. At least one of the first form, the second form, and the third form can comprise a radio signal (e.g., a repeating encoded radio signal).

## Example Authentication/Login Configurations

Various example configurations for authentication/login are described below in accordance with certain embodiments. While each of these descriptions provides an example sequence of steps, these sequences of steps should not be interpreted as limiting, since two or more of the steps can be performed in other sequences relative to one another or can be performed concurrently with one another.

FIG. 7 schematically illustrates a first example configuration for providing a secured authentication/login in accordance with certain embodiments described herein. In certain such embodiments, an electronic device 20 (e.g., a mobile device, smartphone, tablet) can be used to advantageously provide a significantly more secure and faster authentication/login than is conventionally available. The configuration of FIG. 7 shows a minimal number of steps, as compared to the example configurations of FIGS. 8-12, for implementing the authentication/login functionality.

The user can use an electronic device 30 running a user browser with the intention of entering into a secure environment (e.g., to access secure information or sensitive information) hosted by the computer 50 (e.g., a web server). For example, the user can type a secured website uniform resource locator (URL) in a computer browser, although other techniques (e.g., selecting the website from a list of “favorites”) can be used.

The computer 50 can then select the next reusable identifier 214 (e.g., a TSSID which can be the next TSSID of a list of predetermined TSSIDs in a round robin queue) and the corresponding predetermined (e.g., premade) visual or auditory identifier (e.g., a QR code) in which the reusable identifier 214 is encoded. The computer 50 can send a first signal 212 containing the reusable identifier 214 to the verification server 60, and which can indicate the potential beginning of a verification process. The computer 50 can also send a login page signal 702 comprising the selected QR code to the user browser to be displayed to the user. This login page signal 702 can be sent before, concurrently with, or after the first signal 212 is sent.

Using the electronic device 20, the user can scan the QR code (e.g., using the camera of the smartphone) and can extract the reusable identifier 214 (e.g., using a program or application running on the smartphone) to generate a copy 224 of the reusable identifier 214. The electronic device 20 can send a second signal 222 comprising the copy 224 and the user verification information 226 to the verification server 60. The verification server 60 can check the copy 224 and the user verification information 226 it receives from the electronic device 20 against its database (e.g., the first association 232

18

and the second association 234) to determine whether to authorize the user (e.g., authenticate or login the user). For example, authorizing the user can comprise sending an authorization signal 252 (e.g., a valid/invalid flag or authentication information 254) from the validation server 60 to the computer 50.

The computer 50, upon receiving the authorization signal 252, can automatically log in the user and can send a home-page signal 704 to the user browser of the electronic device 30 to display a web page containing, or otherwise allowing access to, the information (e.g., the secured information or the sensitive information) sought to be accessed by the user. In certain embodiments in which the system and method are used to authorize access to a safe, lock or door, upon receiving the authorization signal 252, the safe, lock, or door will open.

FIG. 8 schematically illustrates a second example configuration for providing a secured authentication/login in accordance with certain embodiments described herein. In certain such embodiments, increased security for the authentication/login is provided by adding a user-specific authorization code (e.g., a “personal identification number” or “PIN”) security check (e.g., requiring the user of the electronic device 20 to enter a PIN) to ensure that the authorized user is operating the electronic device 20 and is accessing the secured information. For example, the PIN may be composed of a sequence numbers, a sequence of text characters, or a sequence of images selected from a list of images. The PIN may be static (e.g., user enters the same PIN, until changed) or dynamic (e.g., different authentication questions are asked at different usage points, which may require different user inputs). In certain embodiments described herein, the PINS are user created numeric codes or passwords.

The user can use an electronic device 30 running a user browser with the intention of entering into a secure environment (e.g., to access secure information or sensitive information) hosted by the computer 50 (e.g., a web server). For example, the user can type a secured website uniform resource locator (URL) in a computer browser, although other techniques (e.g., selecting the website from a list of “favorites”) can be used.

The computer 50 can then select the next reusable identifier 214 (e.g., a TSSID which can be the next TSSID of a list of predetermined TSSIDs in a round robin queue) and the corresponding predetermined (e.g., premade) visual or auditory identifier (e.g., a QR code) in which the reusable identifier 214 is encoded. The computer 50 can send a first signal 212 containing the reusable identifier 214 to the verification server 60, and which can indicate the potential beginning of a verification process. The computer 50 can also send a login page signal 702 comprising the selected QR code to the user browser to be displayed to the user. This login page signal 702 can be sent before, concurrently with, or after the first signal 212 is sent.

Upon the user initiating a program running on the electronic device 20, the electronic device 20 can prompt the user to enter a PIN, which the electronic device 20 can verify (e.g., by checking it against a previously setup PIN). If the PIN is correct, the user can then use the electronic device 20 to scan the QR code (e.g., using the camera of the smartphone) and can extract the reusable identifier 214 (e.g., using the program or application running on the smartphone) to generate a copy 224 of the reusable identifier 214. The electronic device 20 can send a second signal 222 comprising the copy 224 and the user verification information 226 to the verification server 60. The verification server 60 can check the copy 224 and the user verification information 226 it receives from the electronic device 20 against its database (e.g., the first association 232

## US 8,677,116 B1

**19**

and the second association 234) to determine whether to authorize the user (e.g., authenticate or login the user). For example, authorizing the user can comprise sending an authorization signal 252 (e.g., a valid/invalid flag or authentication information 254) from the validation server 60 to the computer 50.

The computer 50, upon receiving the authorization signal 252, can automatically log in the user and can send a home-page signal 704 to the user browser of the electronic device 30 to display a web page containing, or otherwise allowing access to, the information (e.g., the secured information or the sensitive information) sought to be accessed by the user. In certain embodiments in which the system and method are used to authorize access to a safe, lock or door, upon receiving the authorization signal 252, the safe, lock, or door will open.

FIG. 9 schematically illustrates a third example configuration for providing a secured authentication/login in accordance with certain embodiments described herein. Besides including the PIN functionality described above with regard to FIG. 8, the electronic device 20 can also receive an authorization signal 706 comprising authorization information 254 from the verification server 60, so that the electronic device 20 can display a successful authorization message to the user.

A user can use an electronic device 30 running a user browser with the intention of entering into a secure environment (e.g., to access secure information or sensitive information) hosted by the computer 50 (e.g., a web server). For example, the user can type a secured website uniform resource locator (URL) in a computer browser, although other techniques (e.g., selecting the website from a list of “favorites”) can be used.

The computer 50 can then select the next reusable identifier 214 (e.g., a TSSID which can be the next TSSID of a list of predetermined TSSIDs in a round robin queue) and the corresponding predetermined (e.g., premade) visual or auditory identifier (e.g., a QR code) in which the reusable identifier 214 is encoded. The computer 50 can send a first signal 212 containing the reusable identifier 214 to the verification server 60, and which can indicate the potential beginning of a verification process. The computer 50 can also send a login page signal 702 comprising the selected QR code to the user browser to be displayed to the user. This login page signal 702 can be sent before, concurrently with, or after the first signal 212 is sent.

Upon the user initiating a program running on the electronic device 20, the electronic device 20 can prompt the user to enter a PIN, which the electronic device 20 can verify (e.g., by checking it against a previously setup PIN). If the PIN is correct, the user can then use the electronic device 20 to scan the QR code (e.g., using the camera of the smartphone) and can extract the reusable identifier 214 (e.g., using the program or application running on the smartphone) to generate a copy 224 of the reusable identifier 214. The electronic device 20 can send a second signal 222 comprising the copy 224 and the user verification information 226 to the verification server 60. The verification server 60 can check the copy 224 and the user verification information 226 it receives from the electronic device 20 against its database (e.g., the first association 232 and the second association 234) to determine whether to authorize the user (e.g., authenticate or login the user). For example, authorizing the user can comprise sending an authorization signal 252 (e.g., a valid/invalid flag or authentication information 254) from the validation server 60 to the computer 50.

The computer 50, upon receiving the authorization signal 252, can automatically log in the user and can send a home-page signal 704 to the user browser of the electronic device 30

**20**

to display a web page containing, or otherwise allowing access to, the information (e.g., the secured information or the sensitive information) sought to be accessed by the user. In certain embodiments in which the system and method are used to authorize access to a safe, lock or door, upon receiving the authorization signal 252, the safe, lock, or door will open. As schematically illustrated by FIG. 9, the verification server 60 can also send an authorization signal 706 comprising authorization information 254 to the electronic device 20.

FIG. 10 schematically illustrates a fourth example configuration for providing a secured authentication/login in accordance with certain embodiments described herein. While including the PIN functionality and the authorization signal 706 described above with regard to FIG. 9, the example configuration of FIG. 10 can have the electronic device 20 transmit the authorization signal 252 comprising the authorization information 254 to the computer 50, instead of the verification server 60 transmitting the authorization signal 252 comprising authorization information 254 to the computer 50. In certain such embodiments, the computer 50 can allow the electronic device 20 to send additional information directly to the computer 50. Alternatively, in certain other embodiments, the computer 50 can send additional information directly to the electronic device 20 (e.g., membership expiration date, urgent actions that need to take place, etc.).

A user can use an electronic device 30 running a user browser with the intention of entering into a secure environment (e.g., to access secure information or sensitive information) hosted by the computer 50 (e.g., a web server). For example, the user can type a secured website uniform resource locator (URL) in a computer browser, although other techniques (e.g., selecting the website from a list of “favorites”) can be used.

The computer 50 can then select the next reusable identifier 214 (e.g., a TSSID which can be the next TSSID of a list of predetermined TSSIDs in a round robin queue) and the corresponding predetermined (e.g., premade) visual or auditory identifier (e.g., a QR code) in which the reusable identifier 214 is encoded. The computer 50 can send a first signal 212 containing the reusable identifier 214 to the verification server 60, and which can indicate the potential beginning of a verification process. The computer 50 can also send a login page signal 702 comprising the selected QR code to the user browser to be displayed to the user. This login page signal 702 can be sent before, concurrently with, or after the first signal 212 is sent.

Upon the user initiating a program running on the electronic device 20, the electronic device 20 can prompt the user to enter a PIN, which the electronic device 20 can verify (e.g., by checking it against a previously setup PIN). If the PIN is correct, the user can then use the electronic device 20 to scan the QR code (e.g., using the camera of the smartphone) and can extract the reusable identifier 214 (e.g., using the program or application running on the smartphone) to generate a copy 224 of the reusable identifier 214. The electronic device 20 can send a second signal 222 comprising the copy 224 and the user verification information 226 to the verification server 60. The verification server 60 can check the copy 224 and the user verification information 226 it receives from the electronic device 20 against its database (e.g., the first association 232 and the second association 234) to determine whether to authorize the user (e.g., authenticate or login the user). For example, authorizing the user can comprise sending an authorization signal 706 (e.g., a valid/invalid flag or authentication information 254) from the validation server 60 to the electronic device 20. The electronic device 20 can then send an

## US 8,677,116 B1

21

authorization signal 252 (e.g., a valid/invalid flag or authentication information 254) to the computer 50.

The computer 50, upon receiving the authorization signal 252, can automatically log in the user and can send a home-page signal 704 to the user browser of the electronic device 30 to display a web page containing, or otherwise allowing access to, the information (e.g., the secured information or the sensitive information) sought to be accessed by the user. In certain embodiments in which the system and method are used to authorize access to a safe, lock or door, upon receiving the authorization signal 252, the safe, lock, or door will open.

FIG. 11 schematically illustrates a fifth example configuration for providing a secured authentication/login in accordance with certain embodiments described herein. While including the PIN functionality described above with regard to FIG. 8, the example configuration of FIG. 11 prompts the user to enter a userID on the electronic device 30 to identify themselves, so that the verification server 60 can send a signal to the appropriate electronic device 20 to ask the user to verify the authentication. This example configuration can be referred to as a “push” configuration since, as described below, a notification is “pushed” from the verification server 60 to the electronic device 20, in contrast to the example configurations of FIGS. 7-10 in which the electronic device 20 transmits a signal comprising the extracted identifier to the verification server 60.

A user can use an electronic device 30 running a user browser with the intention of entering into a secure environment (e.g., to access secure information or sensitive information) hosted by the computer 50 (e.g., a web server). For example, the user can type a secured website uniform resource locator (URL) in a computer browser, although other techniques (e.g., selecting the website from a list of “favorites”) can be used.

The computer 50 can then send a login page signal 702 to the user with a prompt (e.g., a field) to enter the userID of the user. The user can then enter the userID which is then sent by the electronic device 30 to the computer 50 in a signal 708. The userID can comprise of a sequence numbers, text or images selected from a list of images. The userID may be static (e.g., user enters the same userID, until changed) or dynamic (e.g., different authentication questions are asked at different usage points, which may require different user inputs). In certain embodiments described herein, the userIDs are user created numeric codes or passwords. In certain embodiments, the userID can be stored in a cookie on the browser of the electronic device 30, so the userID can be automatically presented to the computer 50.

The computer 50 can then select the next reusable identifier 214 (e.g., a TSSID which can be the next TSSID of a list of predetermined TSSIDs in a round robin queue). The computer 50 can send a first signal 212 containing the reusable identifier 214 and the userID to the verification server 60, and which can indicate the potential beginning of a verification process.

The verification server 60 uses the userID to determine which electronic device 20 corresponds to the userID (e.g., using a stored database or look-up table that correlates the userIDs with corresponding electronic devices 20) and the verification server 60 sends a signal 710 comprising the reusable identifier 214 to the electronic device 20 corresponding to the userID. In response to the signal 710, the electronic device 20 can prompt the user to enter a PIN, which the electronic device 20 can verify (e.g., by checking it against a previously setup PIN). If the PIN is correct, the electronic device 20 can send a second signal 222 comprising the reusable identifier 214 and the user verification information 226 to

22

the verification server 60. The verification server 60 can check the reusable identifier 214 and the user verification information 226 it receives from the electronic device 20 against its database (e.g., the first association 232 and the second association 234) to determine whether to authorize the user (e.g., authenticate or login the user). For example, authorizing the user can comprise sending an authorization signal 252 (e.g., a valid/invalid flag or authentication information 254) from the validation server 60 to the computer 50. In certain embodiments, the verification server 60 can also send an authorization signal 706 comprising authorization information 254 to the electronic device 20.

The computer 50, upon receiving the authorization signal 252, can automatically log in the user and can send a home-page signal 704 to the user browser of the electronic device 30 to display a web page containing, or otherwise allowing access to, the information (e.g., the secured information or the sensitive information) sought to be accessed by the user. In certain embodiments in which the system and method are used to authorize access to a safe, lock or door, upon receiving the authorization signal 252, the safe, lock, or door will open.

FIG. 12 schematically illustrates a sixth example configuration for providing a secured authentication/login in accordance with certain embodiments described herein. While including the PIN functionality described above with regard to FIG. 8, the example configuration of FIG. 12 prompts the user to enter a userID on the electronic device 30 to identify themselves, and the verification server 60 awaits a signal from a securely authenticated user using the electronic device 20 identifying which website to connect to.

A user can use an electronic device 30 running a user browser with the intention of entering into a secure environment (e.g., to access secure information or sensitive information) hosted by the computer 50 (e.g., a web server). For example, the user can type a secured website uniform resource locator (URL) in a computer browser, although other techniques (e.g., selecting the website from a list of “favorites”) can be used.

The webpage reached by the user can include a prompt (e.g., a field) for the user to enter the userID of the user. The user can then enter the userID which is then sent by the electronic device 30 to the computer 50 in a signal 708. The userID can comprise of a sequence numbers, text or images selected from a list of images. The userID may be static (e.g., user enters the same userID, until changed) or dynamic (e.g., different authentication questions are asked at different usage points, which may require different user inputs). In certain embodiments described herein, the userIDs are user created numeric codes or passwords. In certain embodiments, the userID can be stored in a cookie on the browser of the electronic device 30, so the userID can be automatically presented to the website.

The computer 50 can then select the next reusable identifier 214 (e.g., a TSSID which can be the next TSSID of a list of predetermined TSSIDs in a round robin queue). The computer 50 can send a first signal 212 containing the reusable identifier 214 and the userID to the verification server 60, and which can indicate the potential beginning of a verification process.

The verification server 60 uses the userID to determine which electronic device 20 corresponds to the userID (e.g., using a stored database or look-up table that correlates the userIDs with corresponding electronic devices 20) and the verification server 60 sends a signal 710 comprising the reusable identifier 214 to the electronic device 20 corresponding to the userID. In response to the signal 710, the electronic device 20 can prompt the user to enter a PIN, which the

## US 8,677,116 B1

23

electronic device **20** can verify (e.g., by checking it against a previously setup PIN). If the PIN is correct, the user can then use the electronic device **20** to select a website to login (e.g., from a previously-created site list on the electronic device **20**). The electronic device **20** can then send a second signal **222** comprising the address of the selected website, the reusable identifier **214**, and the user verification information **226** to the verification server **60**. The verification server **60** can check the reusable identifier **214** and the user verification information **226** it receives from the electronic device **20** against its database (e.g., the first association **232** and the second association **234**) to determine whether to authorize the user (e.g., authenticate or login the user). For example, authorizing the user can comprise sending an authorization signal **252** (e.g., a valid/invalid flag or authentication information **254**) to the computer **50**. In addition, the verification server **60** can then create an “Authorized Login URL” for the authorized user and can send the “Authorized Login URL” to the computer **50**. The verification server **60** also may send an authorization signal (e.g., a valid/invalid flag or authentication information **254**) to the computer **50**. The computer **50**, upon receiving the authorization signal **252** and the “Authorized Login URL”, can automatically display the “Authorized Login URL” web page containing the user’s information (e.g., the secured information or the sensitive information).

## Example Ecommerce Payment Configurations

Various example configurations for ecommerce payments are described below in accordance with certain embodiments. While each of these descriptions provides an example sequence of steps, these sequences of steps should not be interpreted as limiting, since two or more of the steps can be performed in other sequences relative to one another or can be performed concurrently with one another.

FIG. 13 schematically illustrates a first example configuration for providing a secured electronic payment capability in accordance with certain embodiments described herein. In certain such embodiments, an electronic device **20** (e.g., a mobile device, smartphone, tablet) can be used to advantageously provide a significantly more secure and faster online electronic payment capability than is conventionally available. While described below with reference to websites, the example configurations described below can be used on any payment terminal or a point of sale system for fast and safe payments. The configuration of FIG. 13 shows a minimal number of steps, as compared to the example configurations of FIGS. 14-16, for implementing the electronic payment functionality.

The user can use an electronic device **30** running a user browser with the intention of making a payment. For example, the payment may be made at the end of an online shopping session hosted by the computer **50** (e.g., a web server). The payment process can be initiated by a user clicking on a “checkout” button on a webpage, although other techniques may be used.

The computer **50** can then select the next reusable identifier **214** (e.g., a TSSID which can be the next TSSID of a list of predetermined TSSIDs in a round robin queue) and the corresponding predetermined (e.g., premade) visual or auditory identifier (e.g., a QR code) in which the reusable identifier **214** is encoded. The computer **50** can send a first signal **212** containing the reusable identifier **214** to the verification server **60**, and which can indicate the potential beginning of a payment process. In certain embodiments, in addition to the first signal **212**, the computer **50** also sends information regarding the company, price and shopping cart details to the verification server **60**. The computer **50** can also send a shopping cart page signal **802** comprising the selected QR code to

24

the user browser to be displayed to the user. This shopping cart page signal **802** can be sent before, concurrently with, or after the first signal **212** is sent.

Using the electronic device **20**, the user can scan the QR code (e.g., using the camera of the smartphone) and can extract the reusable identifier **214** (e.g., using a program or application running on the smartphone) to generate a copy **224** of the reusable identifier **214**. The electronic device **20** can send a second signal **222** comprising the copy **224** and the user verification information **226** to the verification server **60**. The verification server **60** can check the copy **224** and the user verification information **226** it receives from the electronic device **20** against its database (e.g., the first association **232** and the second association **234**) to determine whether to authorize the user. For example, authorizing the user can comprise sending an authorization signal **252** (e.g., authentication information **254**, a valid/invalid flag, Boolean true/false, zero/IP address or url of computer **50**) from the validation server **60** to the electronic device **20**. In certain embodiments, the authorization signal **252** comprises at least one of company information, shopping cart information, and information regarding the amount that is to be paid.

The electronic device **20**, upon receiving the authorization signal **252**, can automatically send a payment signal **804** to the computer **50** to provide payment and shipping information to the computer **50**. In certain embodiments, the electronic device **20** can also send an authorization signal (e.g., a valid/invalid flag or authentication information **254**) to the computer **50** as well. The computer **50**, upon receiving the payment signal **804**, can process the payment and can display a receipt page (e.g., by sending a receipt signal **806** to the electronic device **30**).

FIG. 14 schematically illustrates a second example configuration for providing a secured electronic payment capability in accordance with certain embodiments described herein. In certain such embodiments, increased security for the payment is provided by adding a user-specific authorization code (e.g., a “personal identification number” or “PIN”) security check (e.g., requiring the user of the electronic device **20** to enter a PIN) to ensure that the authorized user is operating the electronic device **20** and is completing the transaction. For example, the PIN may be composed of a sequence numbers, text or images selected from a list of images. The PIN may be static (e.g., user enters the same PIN, until changed) or dynamic (e.g., different authentication questions are asked at different usage points, which may require different user inputs). In certain embodiments described herein, the PINs are user created numeric codes or passwords.

The user can use an electronic device **30** running a user browser with the intention of making a payment. For example, the payment may be made at the end of an online shopping session hosted by the computer **50** (e.g., a web server). The payment process can be initiated by a user clicking on a “checkout” button on a webpage, although other techniques may be used.

The computer **50** can then select the next reusable identifier **214** (e.g., a TSSID which can be the next TSSID of a list of predetermined TSSIDs in a round robin queue) and the corresponding predetermined (e.g., premade) visual or auditory identifier (e.g., a QR code) in which the reusable identifier **214** is encoded. The computer **50** can send a first signal **212** containing the reusable identifier **214** to the verification server **60**, and which can indicate the potential beginning of a payment process. In certain embodiments, in addition to the first signal **212**, the computer **50** also sends information regarding the company, price and shopping cart details to the verification server **60**. The computer **50** can also send a shop-

## US 8,677,116 B1

**25**

ping cart page signal **802** comprising the selected QR code to the user browser to be displayed to the user. This shopping cart page signal **802** can be sent before, concurrently with, or after the first signal **212** is sent.

Upon the user initiating a program running on the electronic device **20**, the electronic device **20** can prompt the user to enter a PIN, which the electronic device **20** can verify (e.g., by checking it against a previously setup PIN). If the PIN is correct, the user can then use the electronic device **20** to scan the QR code (e.g., using the camera of the smartphone) and can extract the reusable identifier **214** (e.g., using the program or application running on the smartphone) to generate a copy **224** of the reusable identifier **214**. The electronic device **20** can send a second signal **222** comprising the copy **224** and the user verification information **226** to the verification server **60**. The verification server **60** can check the copy **224** and the user verification information **226** it receives from the electronic device **20** against its database (e.g., the first association **232** and the second association **234**) to determine whether to authorize the user. For example, authorizing the user can comprise sending an authorization signal **252** (e.g., authentication information **254**, a valid/invalid flag, Boolean true/false, zero/IP address or url of computer **50**) from the validation server **60** to the electronic device **20**. In certain embodiments, the authorization signal **252** comprises at least one of company information, shopping cart information, and information regarding the amount that is to be paid.

The electronic device **20**, upon receiving the authorization signal **252**, can automatically send a payment signal **804** to the computer **50** to provide payment and shipping information to the computer **50**. In certain embodiments, the electronic device **20** can also send an authorization signal (e.g., a valid/invalid flag or authentication information **254**) to the computer **50** as well. The computer **50**, upon receiving the payment signal **804**, can process the payment and can display a receipt page (e.g., by sending a receipt signal **806** to the electronic device **30**).

FIG. 15 schematically illustrates a third example configuration for providing a secured electronic payment capability in accordance with certain embodiments described herein. Besides including the PIN functionality described above with regard to FIG. 14, the example configuration of FIG. 15 can provide an additional safety for the user by not sending the sensitive credit card or bank account information to an ecommerce provider (e.g., the computer **50**). Instead, the verification server **60** processes the payment and sends a payment confirmation signal (e.g., flag) to the computer **50**, along with the shipping information. In this way, a user can purchase from an unknown online vendor without risking his credit card or bank account information.

The user can use an electronic device **30** running a user browser with the intention of making a payment. For example, the payment may be made at the end of an online shopping session hosted by the computer **50** (e.g., a web server). The payment process can be initiated by a user clicking on a “checkout” button on a webpage, although other techniques may be used.

The computer **50** can then select the next reusable identifier **214** (e.g., a TSSID which can be the next TSSID of a list of predetermined TSSIDs in a round robin queue) and the corresponding predetermined (e.g., premade) visual or auditory identifier (e.g., a QR code) in which the reusable identifier **214** is encoded. The computer **50** can send a first signal **212** containing the reusable identifier **214** to the verification server **60**, and which can indicate the potential beginning of a payment process. In certain embodiments, in addition to the first signal **212**, the computer **50** also sends information

**26**

regarding the company, price and shopping cart details to the verification server **60**. The computer **50** can also send a shopping cart page signal **802** comprising the selected QR code to the user browser to be displayed to the user. This shopping cart page signal **802** can be sent before, concurrently with, or after the first signal **212** is sent.

Upon the user initiating a program running on the electronic device **20**, the electronic device **20** can prompt the user to enter a PIN, which the electronic device **20** can verify (e.g., by checking it against a previously setup PIN). If the PIN is correct, the user can then use the electronic device **20** to scan the QR code (e.g., using the camera of the smartphone) and can extract the reusable identifier **214** (e.g., using the program or application running on the smartphone) to generate a copy **224** of the reusable identifier **214**. The electronic device **20** can send a second signal **222** comprising the copy **224** and the user verification information **226** to the verification server **60**. The verification server **60** can check the copy **224** and the user verification information **226** it receives from the electronic device **20** against its database (e.g., the first association **232** and the second association **234**) to determine whether to authorize the user. For example, authorizing the user can comprise sending an authorization signal **252** (e.g., authentication information **254**, a valid/invalid flag, Boolean true/false, zero/IP address or url of computer **50**) from the validation server **60** to the electronic device **20**. In certain embodiments, the authorization signal **252** comprises at least one of company information, shopping cart information, and information regarding the amount that is to be paid.

The electronic device **20**, upon receiving the authorization signal **252**, can automatically send a payment signal **804** (e.g., containing payment information, which can include shipping information and/or billing information) to the verification server **60** which process the payment for the ecommerce site. In certain embodiments, the electronic device **20** can also send an authorization signal (e.g., a valid/invalid flag or authentication information **254**) to the verification server **60** as well (e.g., after successfully sending the payment information directly to a payment gateway, causing a payment). The verification server **60**, upon receiving the payment signal **804**, can send a payment confirmation signal **808** (e.g., flag) and the shipping information to the computer **50**. In certain embodiments, the verification server **60** can also send the copy **224** to the computer **50** as well. The computer **50**, upon receiving the payment confirmation signal and the shipping information, can display a receipt page (e.g., by sending a receipt signal **806** to the electronic device **30**).

FIG. 16 schematically illustrates a fourth example configuration for providing a secured electronic payment capability in accordance with certain embodiments described herein. While including the PIN functionality described above with regard to FIG. 14, the example configuration of FIG. 16 prompts the user to enter a userID on the electronic device **30** to identify themselves, so that the verification server **60** can send a signal to the appropriate electronic device **20** to ask the user to verify the payment. This example configuration can be referred to as a “push” configuration since, as described below, a notification is “pushed” from the verification server **60** to the electronic device **20**, in contrast to the example configurations of FIGS. 13-15 in which the electronic device **20** transmits a signal comprising the extracted identifier to the verification server **60**.

The user can use an electronic device **30** running a user browser with the intention of making a payment. For example, the payment may be made at the end of an online shopping session hosted by the computer **50** (e.g., a web

## US 8,677,116 B1

27

server). The payment process can be initiated by a user clicking on a “checkout” button on a webpage, although other techniques may be used.

The computer **50** can then send a checkout or shopping cart page signal **802** to the user with a prompt (e.g., a field) to enter the userID of the user. The user can then enter the userID which is then sent by the electronic device **30** to the computer **50** in a signal **810**. The userID can comprise of a sequence numbers, text or images selected from a list of images. The userID may be static (e.g., user enters the same userID, until changed) or dynamic (e.g., different authentication questions are asked at different usage points, which may require different user inputs). In certain embodiments described herein, the userIDs are user created numeric codes or passwords. In certain embodiments, the userID can be stored in a cookie on the browser of the electronic device **30**, so the user ID can be automatically presented to the computer **50**.

The computer **50** can then select the next reusable identifier **214** (e.g., a TSSID which can be the next TSSID of a list of predetermined TSSIDs in a round robin queue). The computer **50** can send a first signal **212** containing the reusable identifier **214** and the userID to the verification server **60**, and which can indicate the potential beginning of a purchase. In certain embodiments, in addition to the first signal **212**, the computer **50** also sends information regarding the company, price and other details to the verification server **60**.

The verification server **60** uses the userID to determine which electronic device **20** corresponds to the userID (e.g., using a stored database or look-up table that correlates the userIDs with corresponding electronic devices **20**) and the verification server **60** sends a signal **812** comprising the reusable identifier **214** to the electronic device **20** corresponding to the userID. In response to the signal **812**, the electronic device **20** can prompt the user to enter a PIN, which the electronic device **20** can verify (e.g., by checking it against a previously setup PIN). If the PIN is correct, the electronic device **20** can send a second signal **222** comprising the reusable identifier **214** and the user verification information **226** to the verification server **60**. The verification server **60** can check the reusable identifier **214** and the user verification information **226** it receives from the electronic device **20** against its database (e.g., the first association **232** and the second association **234**) to determine whether to authorize the user (e.g., authenticate or login the user). For example, authorizing the user can comprise sending an authorization signal **252** (e.g., authentication information **254**, a valid/invalid flag, Boolean true/false, zero/IP address or url of computer **50**) from the validation server **60** to the electronic device **20**. In certain embodiments, the authorization signal **252** comprises at least one of company information, shopping cart information, and information regarding the amount that is to be paid. In certain embodiments, the verification server **60** can also send an authorization signal **808** comprising authorization information **254** to the computer **50**.

The electronic device **20**, upon receiving the authorization signal **252**, can automatically send a payment signal **804** (e.g., containing payment information, which can include shipping information and/or billing information) to the verification server **60** which process the payment for the ecommerce site. In certain embodiments, the electronic device **20** can also send an authorization signal (e.g., a valid/invalid flag or authentication information **254**) to the verification server **60** as well (e.g., after successfully sending the payment information directly to a payment gateway, causing a payment). The verification server **60**, upon receiving the payment signal **804**, can send a payment confirmation signal **808** (e.g., flag) and the shipping information to the computer **50**. In certain

28

embodiments, the verification server **60** can also send the copy **224** to the computer **50** as well. The computer **50**, upon receiving the payment confirmation signal **808** and the shipping information, can display a receipt page (e.g., by sending a receipt signal **806** to the electronic device **30**).

FIG. 17 schematically illustrates a fifth example configuration for providing a secured electronic payment capability in accordance with certain embodiments described herein. While including the PIN functionality described above with regard to FIG. 14, the example configuration of FIG. 17 sends user validation information **226** to the verification server **60** and payment account information either to the computer **50** or a payment gateway.

The user can use an electronic device **30** running a user browser with the intention of making a payment. For example, the payment may be made at the end of an online shopping session hosted by the computer **50** (e.g., a web server). The payment process can be initiated by a user clicking on a “checkout” button on a webpage, although other techniques may be used.

The computer **50** can then select the next reusable identifier **214** (e.g., a TSSID which can be the next TSSID of a list of predetermined TSSIDs in a round robin queue) and the corresponding predetermined (e.g., premade) visual or auditory identifier (e.g., a QR code) in which the reusable identifier **214** is encoded. The computer **50** can send a first signal **212** containing the reusable identifier **214** to the verification server **60**, and which can indicate the potential beginning of a payment process. In certain embodiments, in addition to the first signal **212**, the computer **50** also sends information regarding the company, price and shopping cart details to the verification server **60**. The computer **50** can also send a shopping cart page signal **802** comprising the selected QR code to the user browser to be displayed to the user. This shopping cart page signal **802** can be sent before, concurrently with, or after the first signal **212** is sent.

Upon the user initiating a program running on the electronic device **20**, the electronic device **20** can prompt the user to enter a PIN, which the electronic device **20** can verify (e.g., by checking it against a previously setup PIN). If the PIN is correct, the user can then use the electronic device **20** to scan the QR code (e.g., using the camera of the smartphone) and can extract the reusable identifier **214** (e.g., using the program or application running on the smartphone) to generate a copy **224** of the reusable identifier **214**. The electronic device **20** can send a second signal **222** comprising the copy **224** and the user verification information **226** to the verification server **60**. The verification server **60** can check the copy **224** and the user verification information **226** it receives from the electronic device **20** against its database (e.g., the first association **232** and the second association **234**) to determine whether to authorize the user. For example, authorizing the user can comprise sending an authorization signal **252** (e.g., authentication information **254**, a valid/invalid flag, Boolean true/false, zero/IP address or url of computer **50**) from the validation server **60** to the electronic device **20**. In certain embodiments, the authorization signal **252** comprises at least one of company information, shopping cart information, and information regarding the amount that is to be paid. In addition, the authorization signal **252** can comprise a payment template to provide information to the electronic device **20** whether payment information is to be sent to the computer **50** or to a separate payment gateway.

The electronic device **20**, upon receiving the authorization signal **252**, can automatically send a payment signal **804** either to the computer **50** or to the separate payment gateway, depending on the payment template provided by the verifica-

## US 8,677,116 B1

29

tion server 60, to provide payment and shipping information. FIG. 17 shows an example in which the payment signal 804 is sent to the computer 50. In certain embodiments, the electronic device 20 can also send a payment confirmation signal 814 (e.g., a valid/invalid flag or authentication information 254) to the verification server 60. In certain embodiments, the payment confirmation signal 814 comprises shipping information. The verification server 60, upon receiving the payment confirmation signal 814, can transmit a payment confirmation signal 808 with the payment confirmation and shipping information to the computer 50. The computer 50 can then display a receipt page (e.g., by sending a receipt signal 806 to the electronic device 30).

## Example Invoice Payment Configurations

Various example configurations for payments of printed invoices are described below in accordance with certain embodiments. While each of these descriptions provides an example sequence of steps, these sequences of steps should not be interpreted as limiting, since two or more of the steps can be performed in other sequences relative to one another or can be performed concurrently with one another.

FIG. 18 schematically illustrates a sixth example configuration for providing a secured electronic payment capability in accordance with certain embodiments described herein. Besides including the PIN functionality described above with regard to FIG. 14, the example configuration of FIG. 18 can provide processing and payment of printed bills, statements, and invoices.

A user can open a bill, statement, or invoice 70, with the intention of making a payment. For example, the invoice 70 can be printed out by the computer 50 and sent to the user. When preparing the invoice 70, the computer 50 can then select the next reusable identifier 214 (e.g., a TSSID which can be the next TSSID of a list of predetermined TSSIDs in a round robin queue) and the corresponding predetermined (e.g., premade) visual identifier (e.g., a QR code) in which the reusable identifier 214 is encoded. By printing the QR code onto the invoice 70 which is to be sent to the user, the computer 50 sends the reusable identifier 214 to the user in a form that can be scanned by the electronic device 20. In addition, the computer 50 can send a first signal 212 containing the reusable identifier 214 to the verification server 60, and which can indicate the potential beginning of a payment process. In certain embodiments, in addition to the first signal 212, the computer 50 also sends information regarding the company, price and other details to the verification server 60.

The payment process proceeds when the user uses the electronic device 20 to scan the visual identifier (e.g., QR code) printed on the invoice 70. Upon the user initiating a program running on the electronic device 20, the electronic device 20 can prompt the user to enter a PIN, which the electronic device 20 can verify (e.g., by checking it against a previously setup PIN). If the PIN is correct, the user can then use the electronic device 20 to scan the QR code (e.g., using the camera of the smartphone) and can extract the reusable identifier 214 (e.g., using the program or application running on the smartphone) to generate a copy 224 of the reusable identifier 214. The electronic device 20 can send a second signal 222 comprising the copy 224 and the user verification information 226 to the verification server 60. The verification server 60 can check the copy 224 and the user verification information 226 it receives from the electronic device 20 against its database (e.g., the first association 232 and the second association 234) to determine whether to authorize the user. For example, authorizing the user can comprise sending an authorization signal 252 (e.g., authentication information 254, a valid/invalid flag, Boolean true/false, zero/IP address or url of computer 50) from the validation server 60 to the electronic device 20. In certain embodiments, the authorization signal 252 comprises at least one of company information and information regarding the amount that is to be paid.

30

or url of computer 50) from the validation server 60 to the electronic device 20. In certain embodiments, the authorization signal 252 comprises at least one of company information and information regarding the amount that is to be paid.

The electronic device 20, upon receiving the authorization signal 252, can automatically send a payment signal 804 (e.g., containing payment information, which can include shipping information and/or billing information) to the verification server 60 which process the payment for the ecommerce site. In certain embodiments, the electronic device 20 can also send an authorization signal (e.g., a valid/invalid flag or authentication information 254) to the verification server 60 as well. The verification server 60, upon receiving the payment signal 804, can send a payment confirmation signal 808 (e.g., flag) and the shipping information to the computer 50. In certain embodiments, the verification server 60 can also send the copy 224 to the computer 50 as well.

FIG. 19 schematically illustrates a seventh example configuration for providing a secured electronic payment capability in accordance with certain embodiments described herein. Besides including the PIN functionality described above with regard to FIG. 14, the example configuration of FIG. 19 can provide processing and payment of printed bills with payment sent directly to the computer 50.

A user can open a bill, statement, or invoice 70, with the intention of making a payment. For example, the invoice 70 can be printed out by the computer 50 and sent to the user. When preparing the invoice 70, the computer 50 can then select the next reusable identifier 214 (e.g., a TSSID which can be the next TSSID of a list of predetermined TSSIDs in a round robin queue) and the corresponding predetermined (e.g., premade) visual identifier (e.g., a QR code) in which the reusable identifier 214 is encoded. By printing the QR code onto the invoice 70 which is to be sent to the user, the computer 50 sends the reusable identifier 214 to the user in a form that can be scanned by the electronic device 20. In addition, the computer 50 can send a first signal 212 containing the reusable identifier 214 to the verification server 60, and which can indicate the potential beginning of a payment process. In certain embodiments, in addition to the first signal 212, the computer 50 also sends information regarding the company, price and other details to the verification server 60.

The payment process proceeds when the user uses the electronic device 20 to scan the visual identifier (e.g., QR code) printed on the invoice 70. Upon the user initiating a program running on the electronic device 20, the electronic device 20 can prompt the user to enter a PIN, which the electronic device 20 can verify (e.g., by checking it against a previously setup PIN). If the PIN is correct, the user can then use the electronic device 20 to scan the QR code (e.g., using the camera of the smartphone) and can extract the reusable identifier 214 (e.g., using the program or application running on the smartphone) to generate a copy 224 of the reusable identifier 214. The electronic device 20 can send a second signal 222 comprising the copy 224 and the user verification information 226 to the verification server 60. The verification server 60 can check the copy 224 and the user verification information 226 it receives from the electronic device 20 against its database (e.g., the first association 232 and the second association 234) to determine whether to authorize the user. For example, authorizing the user can comprise sending an authorization signal 252 (e.g., authentication information 254, a valid/invalid flag, Boolean true/false, zero/IP address or url of computer 50) from the validation server 60 to the electronic device 20. In certain embodiments, the authorization signal 252 comprises at least one of company information and information regarding the amount that is to be paid.

## US 8,677,116 B1

## 31

The electronic device **20**, upon receiving the authorization signal **252**, can automatically send a payment signal **804** (e.g., containing payment information, which can include shipping information and/or billing information) to the computer **50** for processing the payment. In certain embodiments, the electronic device **20** can also send an authorization signal (e.g., a valid/invalid flag or authentication information **254**) to the verification server **60** as well.

FIG. **20** schematically illustrates an eighth example configuration for providing a secured electronic payment capability in accordance with certain embodiments described herein. The example configuration of FIG. **20** is similar to that of FIG. **18** in that it can provide processing and payment of printed bills, statements, and invoices, but it does not utilize the PIN code entry on the electronic device **20** by the user.

A user can open a bill, statement, or invoice **70**, with the intention of making a payment. For example, the invoice **70** can be printed out by the computer **50** and sent to the user. When preparing the invoice **70**, the computer **50** can then select the next reusable identifier **214** (e.g., a TSSID which can be the next TSSID of a list of predetermined TSSIDs in a round robin queue) and the corresponding predetermined (e.g., premade) visual identifier (e.g., a QR code) in which the reusable identifier **214** is encoded. By printing the QR code onto the invoice **70** which is to be sent to the user, the computer **50** sends the reusable identifier **214** to the user in a form that can be scanned by the electronic device **20**. In addition, the computer **50** can send a first signal **212** containing the reusable identifier **214** to the verification server **60**, and which can indicate the potential beginning of a payment process. In certain embodiments, in addition to the first signal **212**, the computer **50** also sends information regarding the company, price and other details to the verification server **60**.

The payment process proceeds when the user uses the electronic device **20** to scan the visual identifier (e.g., QR code) printed on the invoice **70**. By using the electronic device **20** to scan the QR code (e.g., using the camera of the smartphone), the electronic device **20** can extract the reusable identifier **214** (e.g., using the program or application running on the smartphone) to generate a copy **224** of the reusable identifier **214**. The electronic device **20** can send a second signal **222** comprising the copy **224** and the user verification information **226** to the verification server **60**. The verification server **60** can check the copy **224** and the user verification information **226** it receives from the electronic device **20** against its database (e.g., the first association **232** and the second association **234**) to determine whether to authorize the user. For example, authorizing the user can comprise sending an authorization signal **252** (e.g., authentication information **254**, a valid/invalid flag, Boolean true/false, zero/IP address or url of computer **50**) from the validation server **60** to the electronic device **20**. In certain embodiments, the authorization signal **252** comprises at least one of company information and information regarding the amount that is to be paid.

The electronic device **20**, upon receiving the authorization signal **252**, can automatically send a payment signal **804** (e.g., containing payment information, which can include shipping information and/or billing information) to the verification server **60** which process the payment for the ecommerce site. In certain embodiments, the electronic device **20** can also send an authorization signal (e.g., a valid/invalid flag or authentication information **254**) to the verification server **60** as well. The verification server **60**, upon receiving the payment signal **804**, can send a payment confirmation signal **808** (e.g., flag) and the shipping information to the computer **50**. In certain embodiments, the verification server **60** can also send the copy **224** to the computer **50** as well.

## 32

FIG. **21** schematically illustrates a ninth example configuration for providing a secured electronic payment capability in accordance with certain embodiments described herein. The example configuration of FIG. **21** is similar to that of FIG. **19** in that it can provide processing and payment of printed bills, statements, and invoices with payment sent directly to the computer **50**, but it does not utilize the PIN code entry on the electronic device **20** by the user.

A user can open a bill, statement, or invoice **70**, with the intention of making a payment. For example, the invoice **70** can be printed out by the computer **50** and sent to the user. When preparing the invoice **70**, the computer **50** can then select the next reusable identifier **214** (e.g., a TSSID which can be the next TSSID of a list of predetermined TSSIDs in a round robin queue) and the corresponding predetermined (e.g., premade) visual identifier (e.g., a QR code) in which the reusable identifier **214** is encoded. By printing the QR code onto the invoice **70** which is to be sent to the user, the computer **50** sends the reusable identifier **214** to the user in a form that can be scanned by the electronic device **20**. In addition, the computer **50** can send a first signal **212** containing the reusable identifier **214** to the verification server **60**, and which can indicate the potential beginning of a payment process. In certain embodiments, in addition to the first signal **212**, the computer **50** also sends information regarding the company, price and other details to the verification server **60**.

The payment process proceeds when the user uses the electronic device **20** to scan the visual identifier (e.g., QR code) printed on the invoice **70**. By using the electronic device **20** to scan the QR code (e.g., using the camera of the smartphone), the electronic device **20** can extract the reusable identifier **214** (e.g., using the program or application running on the smartphone) to generate a copy **224** of the reusable identifier **214**. The electronic device **20** can send a second signal **222** comprising the copy **224** and the user verification information **226** to the verification server **60**. The verification server **60** can check the copy **224** and the user verification information **226** it receives from the electronic device **20** against its database (e.g., the first association **232** and the second association **234**) to determine whether to authorize the user. For example, authorizing the user can comprise sending an authorization signal **252** (e.g., authentication information **254**, a valid/invalid flag, Boolean true/false, zero/IP address or url of computer **50**) from the validation server **60** to the electronic device **20**. In certain embodiments, the authorization signal **252** comprises at least one of company information and information regarding the amount that is to be paid.

The electronic device **20**, upon receiving the authorization signal **252**, can automatically send a payment signal **804** (e.g., containing payment information, which can include shipping information and/or billing information) to the computer **50** for processing the payment. In certain embodiments, the electronic device **20** can also send an authorization signal (e.g., a valid/invalid flag or authentication information **254**) to the verification server **60** as well.

By using reusable identifiers that do not include user specific or transaction specific information, certain embodiments described herein can advantageously provide a universal login or universal payment application that can work on every website and can provide an exceptional user experience. For example, one smartphone app can be used to log into every website a user wants to access and the user does not have to remember a multitude of passwords for these websites, with different password requirements. This can also save companies a significant amount of money, which would otherwise be spent on customer support services for lost and forgotten passwords. In addition, by utilizing the user verification infor-

## US 8,677,116 B1

**33**

mation that is derived from user-specific or device-specific information, certain embodiments described herein provide a level of safety over a million times greater than systems that utilize just a login and password. Furthermore, in certain embodiments described herein, all the supporting websites will immediately work with the new PIN when a user changes the PIN on his smartphone, and the user does not need to notify any other website, as would be needed for systems that utilize passwords.

Although described above in connection with particular embodiments of the present invention, it should be understood the descriptions of the embodiments are illustrative of the invention and are not intended to be limiting. Various modifications and applications may occur to those skilled in the art without departing from the true spirit and scope of the invention.

What is claimed is:

- 1.** A method of using a computer system to authenticate a user seeking to conduct at least one interaction with a secured capability provided by a computer, the method comprising:
  - using the computer system to receive a first signal from the computer providing the secured capability, the first signal comprising a reusable identifier corresponding to the secured capability, the reusable identifier assigned for use by the secured capability for a finite period of time;
  - using the computer system to receive a second signal from an electronic device being used by the user, the second signal comprising a copy of the reusable identifier and user verification information;
  - using a processor of the computer system to evaluate, based at least on the first signal and the second signal, whether the user is authorized to conduct the at least one interaction with the secured capability; and
  - in response to an indication from the processor that the user is authorized to conduct the at least one interaction with the secured capability, using the computer system to transmit a third signal comprising authorization information to at least one of the electronic device and the computer.
- 2.** The method of claim 1, wherein the reusable identifier does not contain user-specific or interaction-specific information.
- 3.** The method of claim 1, wherein the computer is configured to transmit a fourth signal to a second electronic device being used by the user, the fourth signal comprising the reusable identifier, the second electronic device configured to present the reusable identifier to the user as an encoded visual or auditory identifier configured to be detected by the electronic device and decoded by a program executed by the electronic device to yield the copy of the reusable identifier.
- 4.** The method of claim 3, wherein the second electronic device comprises a visual display and the visual or auditory identifier comprises a QR code.
- 5.** The method of claim 3, wherein the at least one interaction comprises opening a lock selectively inhibiting physical access to a region within a safe, building, or vehicle.
- 6.** The method of claim 3, wherein the at least one interaction comprises retrieval of information from a secured internet portal.
- 7.** The method of claim 3, wherein the at least one interaction comprises a purchase, the first signal further comprises invoice information corresponding to the purchase, the third signal further comprises the invoice information and is transmitted to the electronic device, and the method further comprises receiving, from the electronic device, a confirmation of a payment or payment information corresponding to the purchase by the user.

**34**

**8.** The method of claim 7, wherein the method further comprises transmitting to the computer shipping information for delivery corresponding to the purchase.

**9.** The method of claim 1, wherein the reusable identifier is transmitted to the user on a printed page as a visual identifier configured to be detected by the electronic device and decoded by a program executed by the electronic device to yield the copy of the reusable identifier.

**10.** The method of claim 1, wherein using the processor to evaluate whether the user is authorized to conduct the at least one interaction with the secured capability is based at least on a time differential between receiving the first signal and receiving the second signal.

**11.** A computer system for authenticating users seeking to conduct interactions with a plurality of secured capabilities, the computer system comprising:

a first input configured to receive a plurality of first signals from a plurality of computers, each computer of the plurality of computers providing at least one secured capability of the plurality of secured capabilities, each first signal of the plurality of first signals comprising a reusable identifier corresponding to a secured capability of the plurality of secured capabilities, the reusable identifier assigned for use by the secured capability for a finite period of time;

a second input configured to receive a plurality of second signals from a plurality of electronic devices being used by the users, each second signal of the plurality of second signals comprising a copy of a reusable identifier and user verification information;

a storage device comprising:

a first association of each secured capability of the plurality of secured capabilities with at least one corresponding reusable identifier; and

a second association of the user verification information with corresponding verified users authorized to access at least one secured capability of the plurality of secured capabilities;

a processor configured to evaluate, based at least on a first signal received from a computer of the plurality of computers and a second signal received from an electronic device of the plurality of electronic devices, whether a user of the electronic device is authorized to conduct at least one interaction with a secured capability provided by the computer and corresponding to the reusable identifier; and

an output configured to transmit a third signal comprising authorization information to at least one of the electronic device and the computer providing the secured capability corresponding to the reusable identifier, if the user of the electronic device is authorized to conduct the at least one interaction with the secured capability corresponding to the reusable identifier.

**12.** The system of claim 11, wherein the processor is configured to evaluate, based at least on user verification information of the second signal, whether the user of the electronic device is a verified user.

**13.** The system of claim 11, wherein the processor is further configured to evaluate, based at least on a time differential between receipt of the first signal by the first input and receipt of the second signal by the second input, whether the user is authorized to conduct the at least one interaction with the secured capability corresponding to the reusable identifier.

US 8,677,116 B1

**35**

**14.** The system of claim **11**, wherein the processor is further configured to use the first association and the reusable identifier to identify the secured capability that the user is attempting to access.

**15.** The system of claim **14**, wherein the processor is further configured to use the second association and the user verification information of the second signal received by the second input to determine whether the user is a verified user.

**16.** The system of claim **11**, wherein the reusable identifier does not contain user-specific or interaction-specific information.

**17.** The system of claim **11**, wherein the at least one interaction comprises a purchase, and the first signal further comprises invoice information corresponding to the purchase, wherein the system further comprises a second output configured to transmit the invoice information to the electronic device.

**18.** The system of claim **17**, wherein the second input is further configured to receive a fourth signal from the electronic device comprising a confirmation of a payment or payment information corresponding to the purchase by the user, and the output is configured to transmit the confirmation to the computer.

**19.** The system of claim **18**, wherein the output is further configured to transmit to the computer shipping information for delivery corresponding to the purchase.

**20.** A non-transitory computer storage having stored thereon a computer program that instructs a computer system

5

10

15

20

25

**36**

to authenticate a user seeking to conduct at least one interaction with a secured capability provided by a computer by at least:

receiving a first signal from the computer providing the secured capability, the first signal comprising a reusable identifier corresponding to the secured capability, the reusable identifier assigned for use by the secured capability for a finite period of time;

receiving a second signal from an electronic device being used by the user, the second signal comprising a copy of the reusable identifier and user verification information; using a processor to evaluate, based at least on the first signal and the second signal, whether the user is authorized to conduct the at least one interaction with the secured capability; and

in response to an indication from the processor that the user is authorized to conduct the at least one interaction with the secured capability, transmitting a third signal comprising authorization information to at least one of the electronic device and the computer.

**21.** The method of claim **1**, wherein the computer system comprises the computer providing the secured capability.

**22.** The computer system of claim **11**, wherein the computer system comprises the computer providing the secured capability.

\* \* \* \* \*

UNITED STATES PATENT AND TRADEMARK OFFICE  
**CERTIFICATE OF CORRECTION**

PATENT NO. : 8,677,116 B1  
APPLICATION NO. : 13/963941  
DATED : March 18, 2014  
INVENTOR(S) : Bicer

Page 1 of 1

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the Specification

In column 4 at line 44, Change “nineteenth” to --ninth--.

In column 18 at line 31, Change “PINS” to --PINs--.

In column 19 at line 52, Change “smai phone)” to --smartphone)--.

Signed and Sealed this  
Ninth Day of September, 2014



Michelle K. Lee  
Deputy Director of the United States Patent and Trademark Office